Special issue on secure and privacy-aware data management

Elena Ferrari · Murat Kantarcioglu

Published online: 11 February 2014
© Springer Science+Business Media New York 2014

Recent developments in information systems technologies have resulted in computerizing many applications in various business areas. As a result, data has become a critical asset in many organizations. Even more, amount of data that is generated is exploding. Many applications ranging from social networking to mobile phones create large amounts of potentially sensitive information related to individuals. In addition, recent advances in cloud computing enables the cheap storage and sharing of such large data sets. In many situations, such data could be linked and mined to gain useful insights for creating huge economic and societal value. At the same time, privacy and security concerns can prevent such usage. In addition, further safeguards are needed to build trust in the data, which is instrumental for making critical decisions. To address these challenges, and to capture the full value of large data, we need novel secure and privacy-aware data management solutions.

This special issue presents high quality solution ideas related to the secure and privacy-aware data management challenges occurring in different application domains, such as online social networks, location based applications, data publishing, data outsourcing etc.

The first paper of this issue: *A Generic and Distributed Privacy Preserving Classification Method with A Worst-Case Privacy Guarantee* by Madhushri Banerjee, Zhiyuan Chen and Aryya Gangopadhyay deals with building privacy preserving distributed classification models that are applicable for different classification tasks under worst-case privacy guarantees.

E. Ferrari
University of Insubria, Como, Italy

M. Kantarcioglu (✉)
University of Texas at Dallas, Richardson, TX, USA
e-mail: muratk@utdallas.edu

The second paper: *MILo-DB: a Personal, Secure and Portable Database Machine*, by Nicolas Anciaux, Luc Bouganim, Philippe Pucheral, Yanli Guo, Lionel Le Folgoc, and Shaoyi Yin deals with storing and managing sensitive personal data, such as personal health records using portable hardware devices, such as USB tokens. To overcome the memory and hardware limitations of such hardware, the paper proposes a novel storage and appropriate indexing schemes.

The third paper: *Towards Practical Private Processing of Database Queries over Public Data* by Shiyuan Wang, Divyakant Agrawal, and Amr El Abbadi deals with the privacy issues in querying online services. The paper proposes protocols that provide strong query privacy by using additive homomorphic encryption scheme, and shows how common database queries, such as range and join queries can be answered by relying on the bucketization of public data.

The fourth paper: *Anonymizing Continuous Queries with Delay-tolerant Mix-zones over Road Networks*, by Balaji Palanisamy, Ling Liu, Kisung Lee, Shicong Meng, Yuzhe Tang, and Yang Zhou deals with building a delay-tolerant mix-zones framework to protect the location privacy of mobile device users over road networks. The paper especially addresses the continuous query correlation attacks against location privacy and shows how the proposed techniques can counter against such attacks.

The fifth paper: *An Efficient Privacy-Preserving Multi-Keyword Search over Encrypted Cloud Data with Ranking* by Cengiz Orencik and Erkey Savas deals with efficient secure multi-keyword querying over outsourced sensitive data. The paper proposes an efficient multi-keyword search scheme that ensures users' privacy against both external adversaries, including other authorized users, and cloud server itself. The proposed scheme uses cryptographic techniques as well as query and response randomization to protect user privacy.

The sixth paper: *Detecting and Predicting Privacy Violations in Online Social Networks* by Ozgur Kafali, Akin Gunay, and Pinar Yolum deals with detecting and preventing privacy violations in online social networks. The proposed scheme captures relations among users, their privacy agreements with an online social network operator, the network rules and related meta-data, and applies model checking ideas to detect if relations among the users will result in the violation of privacy agreements.

The seventh paper: *Dynamic Delegation Framework for Role based Access Control in Distributed Data Management Systems*, by Chun Ruan, and Vijay Varadharaja deals with access control and related trusted issues in distributed environments. The paper proposes a logic based framework that extends role based access control systems with dynamic delegation in a decentralized environment. The proposed model also considers the trust issues in role delegation tasks.

Finally, the eight paper: *MetaP: Revisiting Privacy-Preserving Data Publishing using Secure Devices* by Tristan Allard, Benjamin Nguyen, and Philippe Pucheral deals with building a distributed privacy-preserving data publishing platform for sensitive data using secure portable hardware devices. Basically, the proposed solution assumes that the individuals publishing their data are equipped with secure devices and shows how such devices could be used to create anonymized datasets suitable for publishing.

The first six papers are appearing in this special issue. Due to lack of space, last two will appear in the next regular issue. In concluding, we would like to thank all those

that contributed to this special issue: Divy Agrawal, and Amit P. Sheth, the editor-in-chiefs, for their cooperation, the reviewers for their thorough comments that help in enhancing the quality of the papers, and the authors for submitting their papers to this special issue.