
io-port 05799465**Foresti, Sara****Preserving privacy in data outsourcing. Foreword by Pierangela Samarati.**

Advances in Information Security 51. New York, NY: Springer (ISBN 978-1-4419-7658-1/hbk; 978-1-4419-7659-8/ebook). xv, 180 p. EUR 79.95/net; SFR 115.00; \$ 99.00; £ 72.00 (2011).

The author presents a comprehensive approach for protecting sensitive information when it is stored on systems that are not under the data owner's control. The book consists of the following chapters: (1) Introduction; (2) Overview of the state of the art; (3) Selective encryption to enforce access control; (4) Combining fragmentation and encryption to protect data privacy; (5) Distributed query processing under safely composed permissions; (6) Conclusions. Chapter 1 describes motivation, contribution and organization of the book. Chapter 2 discusses the state of the art of the security aspects related to the objectives of the book. It presents the main results obtained in the data outsourcing scenario, focusing on mechanisms for query evaluation, inference exposure measurement, and data integrity. Also, it introduces preliminary works on access control enforcement, privacy protection, and data integration in the considered scenario. Chapter 3 illustrates the access control system for securing data stored at a honest-but-curious server and proposes an efficient mechanism for managing access control policy updates. The risk of collusion among parties is also analyzed to prove the security of the presented solution. Chapter 4 addresses the problem of modeling and enforcing privacy requirements to protect sensitive data and/or their associations. It also presents three cost models for computing an optimal fragmentation, that is, a fragmentation that allows for efficient query evaluation. Chapter 5 focuses on the problem of integrating data made available from different parties and that must satisfy security constraints. It proposes a model for expressing restrictions on data flows among parties and a mechanism for querying distributed data collections under these constraints. Chapter 6 summarizes the contributions of this book and outlines future work. The main contributions can be summarized as follows:

- (1) With respect to the access control enforcement on outsourced data, the original results are: the combined use of selective encryption and key derivation strategies for access control enforcement; the introduction of a notion of minimality of an encryption policy to correctly enforce an access control policy without reducing the efficiency in key derivation; the development of a heuristic approach for computing a minimal encryption policy in polynomial time; the introduction of a two-layer encryption model for the management of policy updates.
- (2) With respect to the definition of a model for enforcing privacy protection, the original results are: the definition of confidentiality constraints as a simple while complete method for modeling privacy requirements; the introduction of the notion of minimal fragmentation that captures the property of a fragmentation to satisfy the confidentiality constraints while minimizing the number of fragments; the development of an efficient approach for computing a minimal fragmentation, which is an NP-hard problem; the introduction of three notions of local optimality, based on the structure of the fragments composing the solution, on the affinity of the attributes in the fragments, and on a query evaluation cost model, respectively; the proposal of three different approaches for computing fragmentations satisfying the three definitions of optimality.
- (3) With respect to the design of a safe data integration mechanism, the original results are: the definition of permissions as a simple while complete method for modeling data exchange limitations; the modeling of both permissions and queries as relation profiles and their representation through a graph-based model; the introduction of an approach for the composition of permissions working in polynomial time; the definition of a method that takes data exchange restrictions into account while designing a query execution plan.

Telman Aliev (Baku)

Keywords: information security; preserving privacy; data protection; sensitive information; encryption; database; access control; distributed query processing

doi:10.1007/978-1-4419-7659-8