Chapter 2.12
An MDA Compliant Approach for Designing Secure Data Warehouses

Rodolfo Villarroel
Universidad Católica del Maule, Chile

Eduardo Fernández-Medina
Universidad de Castilla-La Mancha, Spain

Juan Trujillo
Universidad de Alicante, Spain

Mario Piattini
Universidad de Castilla-La Mancha, Spain

ABSTRACT

This chapter presents an approach for designing secure Data Warehouses (DWs) that accomplish the conceptual modeling of secure DWs independently from the target platform where the DW has to be implemented, because our complete approach follows the Model Driven Architecture (MDA) and the Model Driven Security (MDS). In most of real world DW projects, the security aspects are issues that usually rely on the DBMS administrators. We argue that the design of these security aspects should be considered together with the conceptual modeling of DWs from the early stages of a DW project, and being able to attach user security information to the basic structures of a Multidimensional (MD) model. In this way, we would be able to generate this information in a semi or automatic way into a target platform and the final DW will better suits the user security requirements.

INTRODUCTION

The goal of information confidentiality is to ensure that users can only access to the information that they are allowed. In the case of multidimensional

(MD) models, confidentiality is crucial, because business information that is very sensitive, can be discovered by executing a simple query. Several papers deal with the importance of security in the software development process. Ghosh, Howell, and Whittaker (2002) state that security must influence all aspects of design, implementation, and software tests. Hall and Chapman (2002) put forward ideas about how to build correct systems that fulfil not only the normal requirements but also the security ones. Nevertheless, security in databases and data warehouses is usually focused on the secure data storage, and not on their design. Thus, a methodology of data warehouse design based on the UML, with the addition of security aspects, would allow us to design DWs with the syntax and power of UML and with the new security characteristics ready to be used whenever the application has security requirements that demand them.

In this chapter, we present an approach for designing secure DWs as follows: we define the Model Driven Architecture (MDA) and Model Driven Security (MDS) compliant architecture of our approach, and we provide an Access Control and Audit (ACA) model for the conceptual MD modeling. Then, we extend the Unified Modeling Language (UML) with this ACA model, representing the security information (gathered in the ACA model) in the conceptual MD modeling, thereby allowing us to obtain secure MD models. By using this approach, makes possible to implement the secure MD models with any of the DBMS that are able to implement multilevel databases, such as Oracle Label Security and DB2 Universal Database, UDB.

The remainder of this chapter is structured as follows: Next section introduces related work; next, we present the MDA and MDS compliant architecture of our approach. Finally, we present the main conclusions.

RELATED WORK

As this chapter treats different research topics, the related work is organized as follows.

Multidimensional Modeling

Lately, several MD data models have been proposed. Some of them fall into the logical level (such as the well-known star-schema (Kimball & Ross, 2002). Others may be considered as formal models as they provide a formalism for the consideration of the main MD properties. A review of the most relevant logical and formal models can be found in Blaschka, Sapia, Höfling, and Dinter (1998) and Abelló, Samos, and Saltor (2001).

In this section, we will only make brief reference to the most relevant models that we consider "pure" conceptual MD models. These models provide a high level of abstraction for the main MD modeling properties at the conceptual level and are totally independent from implementation issues. One outstanding feature provided by these models is that they provide a set of graphical notations (such as the classical and well-known Extended Entity-Relationship model) which facilitates their use and reading. These are as follows: *The Dimensional-Fact (DF) Model* by Golfarelli, Maio, and Rizzi (1998), *The Multidimensional/ER (M/ER) Model* by Sapia, Blaschka, Höfling, and Dinter (1998), *The starER Model* by Tryfona, Busborg, and Christiansen (1999), the *Yet Another Multidimensional Model (YAM²)* by Abelló et al. (2001), and the model proposed by Trujillo, Palomar, Gómez, and Song (2001). Unfortunately, none of these approaches for MD modeling considers security as an important issue in their conceptual models, and consequently they do not solve the problem of modeling security from the early stages of a DW project.

Related Content

Data Management and Data Administration: Assessing 25 Years of Practice
Peter Aiken, Mark Gillenson, Xihui Zhangand David Rafner (2011). *Journal of Database Management (pp. 24-45).*
www.irma-international.org/article/data-management-data-administration/55132

An XML Multi-Tier Pattern Dissemination System
Ashraf Gaffarand Ahmed Seffah (2005). *Encyclopedia of Database Technologies and Applications (pp. 740-744).*
www.irma-international.org/chapter/xml-multi-tier-pattern-dissemination/11233

Leveraging Early Aspects in End-to-End Model Driven Development for Non-Functional Properties in Service Oriented Architecture
Hiroshi Wada, Junichi Suzukiand Katsuya Oba (2011). *Journal of Database Management (pp. 93-123).*
www.irma-international.org/article/leveraging-early-aspects-end-end/52994

XML Integration and Toolkit for B2B Applications
Christophe Nicolle, Kokou Yetongnonand Jean-Claude Simon (2003). *Journal of Database Management (pp. 33-58).*
www.irma-international.org/article/xml-integration-toolkit-b2b-applications/3302

Theories of Meaning in Schema Matching: A Review
Joerg Evermann (2008). *Journal of Database Management (pp. 55-82).*
www.irma-international.org/article/theories-meaning-schema-matching/3391