Model Driven Development of Secure XML Data Warehouses: A Case Study

Belén Vela
Rey Juan Carlos University
C/ Tulipán s/n
28933 Móstoles-Madrid , Spain
+34 91 488.70.03
belen.vela@urjc.es

Carlos Blanco
University of Cantabria
Av. De los Castros s/n
39071 Santander, Spain
+34 942 206762
Carlos.Blanco@unican.es

Eduardo Fernández-Medina
University of Castilla-La Mancha
Paseo de la Universidad, 4 – 13071
Ciudad Real, Spain
+34 926 295300
Eduardo.FdezMedina@uclm.es

Esperanza Marcos
Rey Juan Carlos University
C/ Tulipán s/n
28933 Móstoles-Madrid, Spain
+34 91 664.74.91
esperanza.marcos@urjc.es

ABSTRACT
Data Warehouses (DWs) are currently considered to be the cornerstone of Business Intelligence (BI) systems. Security is a key issue in DWs since the business information that they manage is crucial and highly sensitive, and should be carefully protected. However, the increasing amount of data available on the Web signifies that more and more DW systems are considering the Web as the primary data source through which to populate their DWs. XML is therefore widely accepted as being the principal means through which to provide easier data and metadata interchange among heterogeneous data sources from the Web and the DW systems.
Although security issues have been considered during the whole development process of traditional DWs, current research lacks approaches with which to consider security when the target platform is based on the Web and XML technologies. The idiosyncrasy of the unstructured and semi-structured data available on the Web definitely requires particular security rules that are specifically tailored to these systems in order to permit their particularities to be captured correctly.
In order to tackle this situation, in this paper, we propose a methodological approach based on the Model Driven Architecture (MDA) for the development of Secure XML DWs. We therefore specify a set of transformation rules that are able to automatically generate not only the corresponding XML structure of the DW from secure conceptual DW models, but also the security rules specified within the DW XML structure, thus allowing us to implement both aspects simultaneously. A case study is provided at the end of the paper to show the benefits of our approach.

Keywords
Secure XML Data Warehouse, Model Driven Development, MDA, XML.

EDBT 2010, March 22–26, 2010, Lausanne, Switzerland.

1. INTRODUCTION
Data Warehouse (DW) systems provide a Multidimensional (MD) view of huge amounts of historical data from heterogeneous operational sources, thus supplying useful and sensitive information which allows decision makers to improve business processes in organizations. The MD paradigm structures information into facts and dimensions. A fact contains the interesting measures (fact attributes) of a business process (sales, deliveries, etc.), whereas a dimension represents the context for analyzing a fact (product, customer, time, etc.) by means of hierarchically organized dimension attributes.

Traditional DW systems allow business people to acquire useful knowledge from their organization's data by means of a variety of technologies, such as OLAP or data mining. However, in order to provide richer insights into the dynamics of today's business, it is currently desired that the data inside the organization be combined with data from the outside, thus complementing the company's internal data with value-adding information (e.g., retail prices of products sold by competitors). Since the amount of data available on the Web has been growing rapidly over the last decade, Web data prove to be more and more useful for this purpose. The main problem with data from the Web is that they are rather heterogeneous and complex. To overcome such drawbacks, designers of DW systems make use of this data by using XML technologies [19,23]. On the one hand, Web warehousing uses XML as a means of ameliorating the extraction and integration of heterogeneous Web data in the DW [10]. On the other hand, document warehousing requires XML to deal with unstructured data in DW systems [24]. In both cases XML is used to implement the MD model underlying the DW by defining the corresponding design artifacts (facts, dimensions, measures, hierarchies and so on) in order to facilitate the interchange of data and metadata among heterogeneous data sources and the DW system [29]. The design of XML DWs is therefore a cornerstone when it is necessary to use Web data in the decision making process, which is becoming more and more frequent.

Furthermore, every design issue should be considered in the development process of an XML DW. Specifically, one of the

most important design issues is security, which has, to date, been surprisingly overlooked when XML DWs are being developed. Considering that the information managed by DWs is frequently highly sensitive, and sometimes refers to personal data (protected under the law in most countries), DWs should be protected from unauthorized information accesses (whatever the implementation platform is). In fact, a key requirement underlying these recently developed data management systems is a demand for adequate security, and fine-grained flexible authorization models and access control mechanisms (since DWs deal mainly with read operations). Therefore, rather than considering security once the system has been completely built, we believe that security and privacy measures should be integrated in all layers of the DW design, from the early stages of its development as another relevant requirement, meaning that much more robust, secure and platform independent products will be produced [19,31].

In order to develop secure XML DWs considering confidentiality issues in the whole development process, from an early development stage to the final implementation, our proposal has been aligned with an MDA (Model Driven Architecture [20]) architecture in which security models are embedded in and scattered throughout the high level system models, which are transformed until their final implementation according to the MDA strategy. MDA can be used for this purpose, since it shares some similarities with the traditional MD modeling methods [27]: i) a conceptual design phase is carried out, whose output is an implementation-independent and expressive conceptual MD model for the DW (i.e. a Platform Independent Model, PIM), ii) a logical design phase aims to obtain a technology-dependent model (i.e. a Platform Specific Model, PSM) from the previously defined conceptual MD model, and iii) this logical model is then the basis for the implementation of the DW.

After presenting some related works in the following section, in Section 3 we will introduce the secure XML DW development approach. The PIM is the secure conceptual DW data model, which will be semi-automatically transformed into a secure XML DW, as a PSM, applying a set of transformation rules summarized in Section 4. In addition, in Section 5 we will present a case study to show our proposal. Finally, in Section 6, we will put forward our main conclusions and present our future work.

2. RELATED WORK

In this section the related work is organized according to the following topics: (1) MD modeling, (2) security integration into the design process and (3) security and access control models for DWs.

2.1 MD Modeling

Some MD data models are focused on the logical level [1,6]. However, the most interesting proposals consider the conceptual level in order to model multidimensional concepts (facts, dimensions, classification hierarchies and so on) in a platform independent manner by extending the classical EER model [30,32] by defining their own graphical notation [11,13]. On the other hand, other proposals use the object-oriented paradigm and are based on UML (YAM2 [2] or the object oriented metacube [5]).

Furthermore, when dealing with XML DWs, some works model and analyze this kind of systems by taking into account the fact that cubes and dimensions are stored in XML documents [7,22] and extend the XQuery language with OLAP capabilities [4,12,38]. All of these modeling proposals permit the definition of DWs' structural aspects, but only some of them (ADAPTed UML [26] and SECDW [8]) consider security as an important issue to be considered in DW modeling, although they do not deal with XML data warehousing.

2.2 Secure Integration into the design process

Several relevant works can be found which concern a complete secure development but which focus on information systems in general. For instance, UMLSec [14] uses UML to define and evaluate security specifications using formal semantics. Moreover, Model Driven Security (MDS) [3] uses the MDA approach to include security properties in high-level system models and to automatically generate secure system architectures. Within the context of MDS, SecureUML [17] is proposed as an extension of UML for modeling a generalized role based access control. On the other hand, Mokum [33] is an active object oriented knowledge base system for modeling, which permits the specification of security and integrity constraints and automatic code generation. These are relevant contributions towards secure information systems development but are not specifically focused on DWs.

2.3 Security and Access Control Models for DWs

Since final users work with an MD model when querying a DW (facts, dimensions, classification hierarchies, etc.), security constraints must be defined in terms of MD modeling.

There are several interesting initiatives for the inclusion of security in DWs, but they are not conceived for integration into MD modeling as part of the DW design process, and, inconsistent security measures may consequently be defined. Katic et al. [15] present a security model based on metadata to define user groups and views. Rosenthal and Sciore [27] integrate security from the data sources and propagate it to DW design. Other proposals define authorization models and security for DWs [16,25,26,36,37] but they deal solely with OLAP operations (such us roll-up or drill-down).

3. SECURE XML DW MODELING

In this paper, we use the Model Driven Architecture (MDA) [20] to define security in the MD modeling of XML DWs. We concretely define security specifications in the Conceptual MD Data Model (PIM), independently of the target logical MD model. This Secure Conceptual MD Data Model will be used as a starting point and will be semi-automatically transformed into a Secure XML DW as a logical model (PSM) by applying Model to Model (M2M) Transformations. Finally, a Model to Text (M2T) transformation will generate the code for the Secure XML DW.

For the model driven development of a secure XML DW it is therefore necessary to perform the following tasks (see Figure 1):

- At the **PIM level**, the secure MD data model is carried out without considering the selected technology, since this model is independent of the platform. This MD PIM (described in more detail in the following subsection) is represented through an extended UML class diagram for DWs which furthermore permits the specification of security constraints on the model.

- At the **PSM level**, the data logical design is performed, taking into account the selected target platform in which the DW will be implemented. In our case, XML technology will be used for the implementation of the DW in any secure commercial database management system. We shall start from the secure MD PIM obtained at the previous level and shall apply the mappings summarized in Section 4 to obtain an XML Schema, conforming to the XML Schema Metamodel [35].

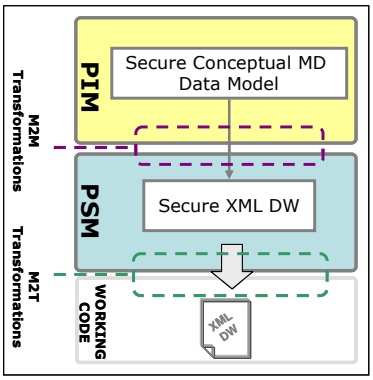

Figure 1. Development approach for Secure XML DW

3.1 Secure MD PIM

As previously mentioned, our proposed development approach starts from the conceptual model of the secure MD PIM.

In order to define this secure MD PIM, a secure UML profile denominated as SECDW has been developed (for more details, see [8]). SECDW (Figure 2) considers both specific aspects of DW modeling (such as facts, dimensions, base classes, measures, hierarchies, many-to-many relations, degenerated dimensions, multiple classifications or alternative paths of hierarchies) and security capabilities by using an Access Control and Audit (ACA) model [9].

The ACA model classifies authorization subjects and objects into security roles ("*SRole*" metaclass) which organize users into a hierarchical role structure according to the responsibilities of each type of work, levels ("*SLevel*" metaclass) which indicate the user's clearance level, and compartments ("*SCompartment*" metaclass) which classify users into a set of horizontal compartments or groups.

The definition of several kinds of security rules related to the multidimensional elements of DWs is also permitted: Sensitive Information Assignment Rules (SIAR) ("*SecurityRule*" metaclass) which specify multilevel security policies and allow sensitive information to be defined for each element in the multidimensional model; Authorization Rules (AUR) ("*AuthorizationRule*" metaclass) which permit or deny access to certain objects by defining the subject that the rule applies to, the object that the authorization refers to, the action that the rule refers to and the sign describing whether the rule permits or denies access; and Audit Rules (AR) ("*AuditRule*" metaclass) which ensure that authorized users do not misuse their privileges.

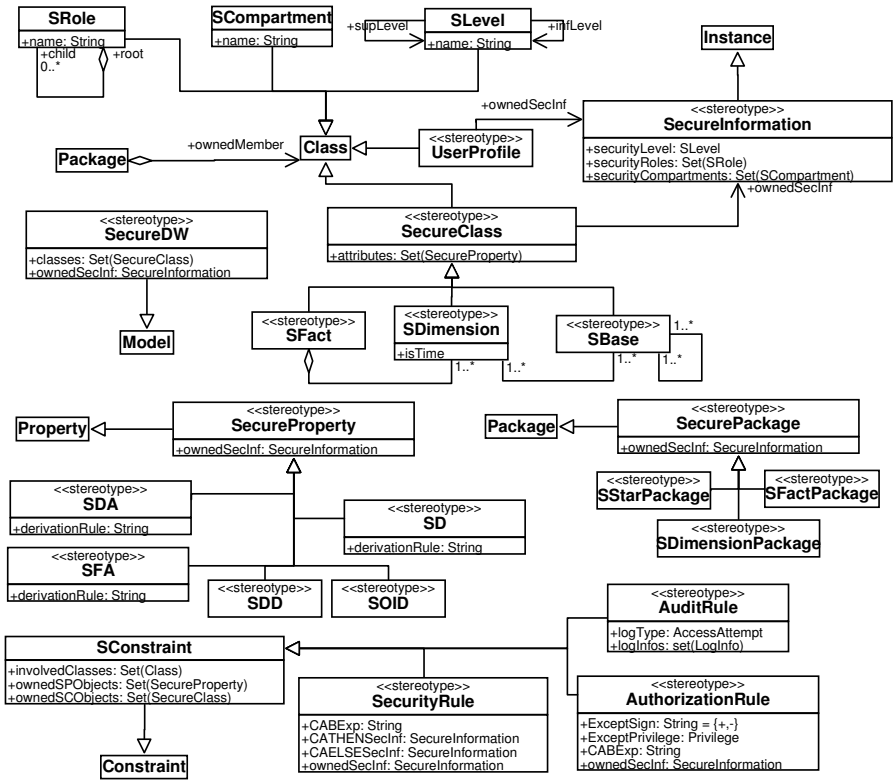

Figure 2. Conceptual Secure MD Metamodel

4. Mappings from PIM to PSM

In the same way that methodologies for relational or OR DBs propose certain rules for the transformation of a conceptual schema into a logical schema, in this section we propose the mappings from the secure MD PIM to the XML Schema for the Secure XML DW. The basis for this is the work of [34], in which the different mappings used to obtain the schema of a secure XML DB were defined but did not take into consideration security aspects for MD modeling aspects. Table 1 shows the mapping rules for the transformation of a secure multidimensional model (PIM level) into an XML Schema model (PSM level).

Table 1. PIM to PSM Tranformation Rules

Data PIM	Data PSM
Secure MD PIM	XML Schema which includes the root element "SecureMDXML" of "SecureMDXML_Type", which includes the Star Packages, Security Levels, Security Roles Hierarchy, Security Compartments and User Profile.
Security Levels	XML Element named "SecurityLevels" including a sequence complexType (SecurityLevel_Type) with all the defined Security Levels as subelements. Each subelement will contain the subelements: *name*, *short name* and *order number* (beginning with 1, as the *highest* security level).
Security Roles *Hierarchy*	XML Element named "SecurityRoles" including a sequence complexType (SecurityRole_Type) with all the defined Security Levels as subelements. Each subelement will contain the *name* and a reference element to its parent, that is, the security role which includes it.
Security Compartments	XML Element named "SecurityCompartments" including a sequence complexType (SecurityCompartments_Type) with all the defined Security Compartments as subelements.
Secure Information *Class* SecurityLevels SecurityRoles securityCompartments	XML ComplexType named "SecureInformationType" with three subelements: • *SecurityLevels of SecurityLevel_Type with the corresponding attributes as XML subelements* • *SecurityRoles of SecurityRoles_Type with the corresponding attributes as XML subelements* • *securityCompartments of SecurityCompartments_Type with the corresponding attributes as XML subelements*
User Profile *Class*	XML Element of a sequence complexType "UserProfile_Type" which includes as subelements its code, the name, the specific class attributes and the SecureInformation subelement of SecureInformation_Type.
Secure Star Package	XML Element named "StarPackage" including a complexType with the Fact, Dimension and Base XML Subelements, each of which contains the corresponding Security Information and Security Constraints as XML Subelements.
Classes *Attribute of PIM* *classes* OID	XML Element of complexType including references to all the elements transformed from the PIM classes XML Subelement of complexType
Secure Base *Class*	XML Subelement (*of the StarPackage*) including the OID attribute, a sequence complexType with all class Descriptor and Dimension attributes
OID	XML attribute of ID type of the element
Descriptor	XML Subelement of complexType
Dimension	XML Subelement of complexType
Secure Fact *Class*	XML Subelement (*of the StarPackage*) including the OID attribute, a sequence complexType with the Fact attributes
OID	XML attribute of ID type of the element
Fact	XML Subelement of the complexType
Secure Dimension *Class*	XML Subelement (*of the StarPackage*) including the OID attribute, a sequence complexType with all class, Descriptor and Dimension attributes. This also includes an attribute of IDREF type named as the base class + "_Base_Ref", which includes a reference to the base class element with which it is associated.
OID	XML attribute of ID type of the element
Descriptor	XML Subelement of the complexType
Dimension	XML Subelement of the complexType
Secure Class *Attributes*	XML Subelement including the class attribute and the security properties

Association	
securityLevels attribute	XML Subelement of the association element (maxOccurs=unbounded)
securityRoles attribute	XML Subelement of the association element
securityCompartments at.	XML Subelement of the association element (maxOccurs=unbounded)
Constraint • involvedClasses • ownedSPObjects • ownedSCObject	XML Subelement of the corresponding base, dimension or fact element with three optional attributes (involvedObjects, ownedSPObjects, ownedSCObjects), with references to the elements, secure properties or secure elements.
AuditRule	- AuditRuleType of simpleType with enumeration constraint - AuditRuleCondition of string type containing the XPath expression associated with the OCL expression
AuthorizationRule	- AuthorizationRuleSign of simpleType with enumeration constraint {+,-} - Privileges of simpleType with enumeration constraint - AuthorizationRuleCondition of string type that will contain the XPath expression associated with the OCL expression
SecurityRule	- Subelement of complexType with three subelements of string type • CABExp that will contain the expression in XPATH • CATHEN that will contain the Security Information if the expression is TRUE • CAELSE that will contain the Security Information if the expression is FALSE

5. CASE STUDY

This section presents an example based on an airport DW that manages information concerning trips, flights and incidents, in which the XML secure model (PSM) is obtained from the secure conceptual MD data model (PIM).

Figure 3 shows a partial view of the multidimensional model focused on trip information (secure fact class "Trip") involving passengers (secure dimension class "Passenger") who take flights to reach their destinations (secure dimension class "Place" and a related secure base class "Airport"). Some attributes have been included to manage information about trips (price, purpose, seat, distance, flight time, and whether or not checking in and boarding have taken place), departure and arrival locations (gate, terminal and airport), and passengers (personal data: name and address; and security information: fingerprints, photo and whether or not the passenger is considered to be suspicious).

In order to establish security constraints, a security configuration has been defined by using security levels (SL) and security roles (SR). The security levels are top secret (TS), secret (S), confidential (C) and unclassified (U), and the hierarchy of security roles is composed of a main role "User" with three subroles "Airport Security", "Administration" and "Passenger". A set of sensitive information assignment rules (SIAR) has then been defined over some classes and attributes by using stereotypes. The "Trip" fact class and the "Place" dimension class can be accessed by users with the confidential (or upper) security level; the "Passenger" dimension by those with the secret security level; and the "Airport" dimension by those with the undefined security level. Several attributes also have fine grain security constraints associated with them, which permit the security role "Airport Security" to access the attributes: "purpose" (of the "Trip" fact), and "fingerprints", "passportPhoto" and "suspicious" (of the "Passenger" dimension).

More complex security (SIAR) and authorization (AUR) rules have also been defined by using the metaclasses "SecurityRule" and "AuthorizationRule". The "SIAR_TripPurpose" rule is associated with the "Trip" fact and involves the "Passenger" dimension. This rule increases the security requirements of the fact and the involved classes if the purpose of the trip is military ("purpose" attribute). In this case a security level of "Secret" and a security role of "Airport Security" will be required. The "AUR_Passenger" is a positive authorization rule which checks the user name ("name" attribute of "UserProfile") and provides access to his/her passenger information.

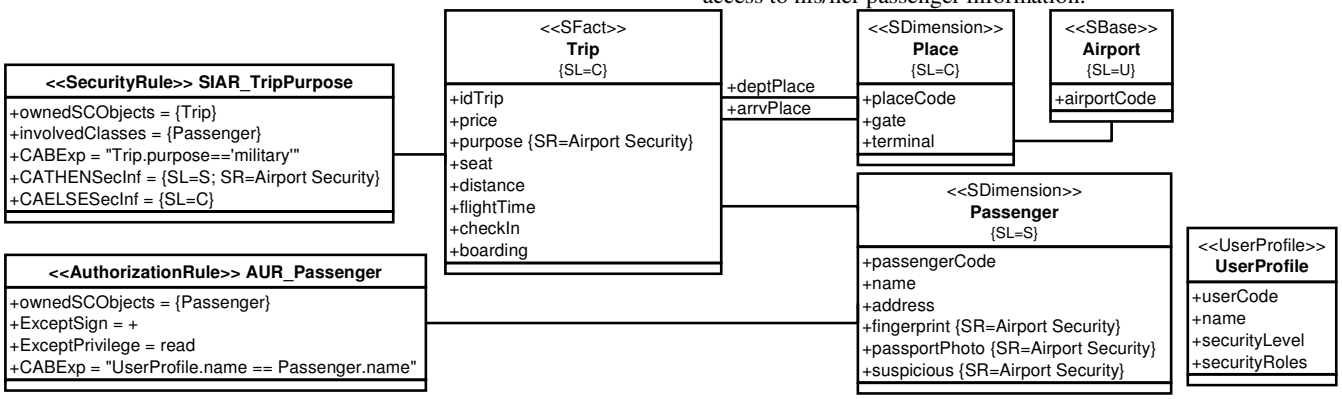

Figure 3. PIM model for Airport example

We have used this Secure MD PIM as a starting point to apply the defined transformation rules and we have obtained the following XML Schema. Only a part of the generated XML PSM is shown owing to space constraints.

```
<?xml version="1.0" encoding="utf-8" ?>
- <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <xs:element name="SecureMDXML" type="SecureMDXML_Type" />
+ <xs:complexType name="SecureInformation_Type">
+ <xs:complexType name="UserProfile_Type">
- <xs:complexType name="StarPackage_Type">
- <xs:sequence>
+ <xs:element name="SecureBaseClasses">
- <xs:element name="SecureFactClasses">
- <xs:complexType>- <xs:sequence>
- <xs:element name="Trip" maxOccurs="unbounded">
- <xs:complexType>- <xs:sequence>
  <xs:element name="SecurityLevel" fixed="C" />
  <xs:element name="price" type="xs:integer" />
- <xs:element name="purpose">
- <xs:complexType>- <xs:sequence>
  <xs:element name="S_purpose" type="xs:string" />
        <xs:element name="SecurityRole" type="xs:string" fixed="AirportSecurity" />
  </xs:sequence> </xs:complexType> </xs:element>
  <xs:element name="seat" type="xs:string" />
  <xs:element name="distance" type="xs:string" />
  <xs:element name="flightTime" type="xs:string" />
  <xs:element name="checkIn" type="xs:string" />
  <xs:element name="boarding" type="xs:string" />
- <xs:element name="SecurityRules">
- <xs:complexType>- <xs:sequence>
- <xs:element name="SIAR_TripPurpose">
- <xs:complexType>- <xs:sequence>
          <xs:element name="CABEXP" type="xs:string" fixed="Trip.purpose==military" />
- <xs:element name="CABTHEN">
- <xs:complexType>- <xs:sequence>
        <xs:element name="SecurityLevel" type="xs:string" fixed="AirportSecurity" />
  <xs:element name="SecurityRole" type="xs:string" fixed="S" />
  </xs:sequence> </xs:complexType>
  </xs:element>
- <xs:element name="CABELSE" minOccurs="0">
- <xs:complexType>- <xs:sequence>
  <xs:element name="SecurityRole" type="xs:string" fixed="C" />
  </xs:sequence> </xs:complexType> </xs:element> </xs:sequence>
  <xs:attribute name="ownedSCObjects" fixed="Trip" />
  <xs:attribute name="involvedClasses" fixed="Passenger" />
  </xs:complexType> </xs:element> </xs:sequence>
  <xs:attribute name="idTrip" type="xs:ID" />
  </xs:complexType> </xs:element>
  </xs:sequence> </xs:complexType> </xs:element>
  </xs:sequence> </xs:complexType> </xs:element>
- <xs:element name="SecureDimensionClasses">
- <xs:complexType>- <xs:sequence>
- <xs:element name="Place" maxOccurs="unbounded">
```

```
- <xs:complexType>- <xs:sequence>
  <xs:element name="SecurityLevel" fixed="C" />
  <xs:element name="gate" type="xs:string" />
  <xs:element name="terminal" type="xs:string" />
  </xs:sequence> <xs:attribute name="placeCode" type="xs:ID" />
  <xs:attribute name="AirPort_Base_Ref" type="xs:IDREF" />
  </xs:complexType> </xs:element>
- <xs:element name="Passenger" maxOccurs="unbounded">
- <xs:complexType>- <xs:sequence>
  <xs:element name="SecurityLevel" fixed="S" />
  <xs:element name="name" type="xs:string" />
  <xs:element name="address" type="xs:string" />
- <xs:element name="fingerprint">- <xs:complexType>- <xs:sequence>
  <xs:element name="S_fingerprint" type="xs:string" />
        <xs:element name="SecurityRole" type="xs:string" fixed="AirportSecurity" />
  </xs:sequence> </xs:complexType> </xs:element>
- <xs:element name="passportPhoto">
- <xs:complexType>- <xs:sequence>
  <xs:element name="S_passportPhoto" type="xs:string" />
        <xs:element name="SecurityRole" type="xs:string" fixed="AirportSecurity" />
  </xs:sequence> </xs:complexType> </xs:element>
- <xs:element name="suspected">
- <xs:complexType>- <xs:sequence>
  <xs:element name="S_suspected" type="xs:string" />
        <xs:element name="SecurityRole" type="xs:string" fixed="AirportSecurity" />
  </xs:sequence> </xs:complexType> </xs:element>
- <xs:element name="AutorizationRules">
- <xs:complexType>- <xs:sequence>
- <xs:element name="AUR_Passenger">
- <xs:complexType>- <xs:sequence>
  <xs:element name="Sign" type="xs:string" fixed="+" />
  <xs:element name="Privilege" type="xs:string" fixed="read" />
  <xs:element name="CABEXP" type="xs:string" fixed="UserProfile.name==Passenger.name" />
    <xs:element name="SecInf" type="SecureInformation_Type" minOccurs="0" />
  </xs:sequence>
  <xs:attribute name="ownedSCObjects" fixed="Passenger" />
  </xs:complexType>
 </xs:element>
</xs:sequence>
</xs:complexType> </xs:element> </xs:sequence>
  <xs:attribute name="passengerCode" type="xs:ID" />
  </xs:complexType>
  </xs:element>
  </xs:sequence>
  </xs:complexType>
  </xs:element>
  </xs:sequence>
</xs:complexType>
- <xs:complexType name="SecureMDXML_Type">
```

```
- <xs:sequence>
- <xs:element name="UserProfiles">
- <xs:complexType>
- <xs:sequence>
    <xs:element name="UserProfile" type="UserProfile_Type" maxOccurs="1" />
  </xs:sequence>
 </xs:complexType>
</xs:element>
  <xs:element name="StarPackage" type="StarPackage_Type" />
  </xs:sequence>
</xs:complexType>
  </xs:schema>
```

Figure 4. PSM XML Schema Model for the Airport example

6. CONCLUSIONS AND FUTURE WORKS

In this work we have proposed an approach for the model driven development of Secure XML DWs. Our approach starts by defining the secure conceptual MD model (PIM) represented by means of the secure UML profile called SECDW, independently of the target logical MD model. This PIM is used as a starting point and is then semi-automatically transformed into a secure XML DW, as a logical model (PSM), by applying Model to Model (M2M) Transformations. In this paper, we have specified these transformation rules with which to automatically generate not only the corresponding XML structure of the DW from the secure conceptual models of the DW, but also the security rules specified within the DW XML structure, thus allowing both aspects to be implemented simultaneously.

In order to validate our proposal we have carried out several case studies. One of these is shown in this paper to illustrate the benefit of our approach: an airport DW that manages information concerning trips, flights and incidents.

We are now working on several different lines, in an attempt to extend the proposal presented in this paper. One of these, on which we have already started to work, is the automation of the transformations of the constraints expressed in OCL at the PIM level, in order to convert them into XPATH language. Moreover, we are also working on the automation of the transformations between the metamodels and the corresponding models using the Query View Transformation (QVT) proposal [21]. A further goal is that of performing several case studies to detect new needs. These would also analyze the advantages of incorporating security aspects provided by the different XML DB administrators, and not only those which are native. The next step, will be to include our proposal in the case tool that we are developing for the semi-automatic development of Secure XML DW.

7. ACKNOWLEDGMENTS

This research has been carried out in the framework of the following projects: MODEL-CAOS (TIN2008-03582/TIN) and AGREEMENT-TECHNOLOGY (CSD2007-0022) financed by the Spanish Ministry of Education and Science, IDONEO (PAC08-0160-6141) financed by the "Consejería de Ciencia y Tecnología of the Junta de Comunidades de Castilla-La Mancha", the Data Management network (TIN2008-04453-E), financed by the Spanish Ministry of Science and Innovation (MCI), the BUSINESS (PET2008-0136) financed by the MCI, the QUASIMODO (PAC08-0157-0668) financed by the "Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha" and the SISTEMAS (PII2I09-0150-3135) financed by the "Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha".

8. REFERENCES

[1] Abelló, A., J. Samos, and Saltor, F. A Framework for the Classification and Description of Multidimensional Data Models. In: 12th Int. Conference on Database and Expert Systems Applications (DEXA'01). LNCS 2113: p. 668-677, 2001.

[2] Abelló, A., J. Samos, and Saltor, F. YAM2: a multidimensional conceptual model extending UML. Information Systems. 31(6): p. 668-677, 2006.

[3] Basin, D., J. Doser, and Lodderstedt, T. Model Driven Security: from UML Models to Access Control Infrastructures. ACM Transactions on Software Engineering and Methodology. 15(1): p. 39-91, 2006.

[4] Beyer, K.S., et al., Extending XQuery for Analytics. In: ACM SIGMOD Int. Conference on Management of Data. 2005: Baltimore, Maryland. p. 503-514.

[5] Binh, N.T., Tjoa, A.M. and Wagner, R. An object oriented multidimensional data model for OLAP, in Web-Age Information Management. 2000. p. 69-82.

[6] Blaschka, M., Sapia, G. Höfling, B. and Dinter, Finding your way through multidimensional data models. In: 9th Int. Conf. on Database and Expert Systems Applications (DEXA'98). LNCS1460, 1998.

[7] Boussaid, O., Messaoud, R.B., Choquet, R. and Anthoard, S., X-Warehousing: An XML-Based Approach for Warehousing Complex Data, In: 10th East-European Conference on Advances in Databases and Information Systems ADBIS 2006, Springer Verlag: Thessaloniki, Greece. p. 39-54.

[8] Fernández-Medina, E., Trujillo, J., Villarroel, R. and Piattini, M. Developing secure data warehouses with a UML extension. Information Systems, 2007. 32(6): p. 826-856.

[9] Fernández-Medina, E., Trujillo, J., Villarroel, R. and Piattini, M. Access Control and Audit Model for the Multidimensional Modeling of Data Warehouses. Decision Support Systems, 2006. 42: p. 1270-1289.

[10] Golfarelli, M., S. Rizzi, and Vrdoljak, B.Data Warehouse Design from XML Sources. DOLAP 2001.

[11] Golfarelli, M., Maio, D. and Rizzi, S. The Dimensional Fact Model: A Conceptual Model for Data Warehouses. Int. Journal of Cooperative Information Systems (IJCIS). 7.(2-3): p. 215-247, 1998.

[12] Hachicha, M., Mahboubi, H. and Darmont, J. Expressing OLAP operators with the TAX XML algebra, in EDTB workshop on Database Technologies for Handling XML

Information on the Web (DataX-EDBT). 2008: Nantes, France. p. 61-66.

[13] Husemann, B., Lechtenborger, J. and Vossen, G. Conceptual Data Warehouse Design, In DMDW'2000. 2000, Technical University of Aachen (RWTH): Stockholm, Sweden. p. 3-9.

[14] Jürjens, J., Secure Systems Development with UML. 2004: Springer-Verlag.

[15] Katic, N., Quirchmay, G., Schiefer, J., Stolba, M. and Tjoa, A.M. A Prototype Model for Data Warehouse Security Based on Metadata. In 9th Int. Workshop on Database and Expert Systems Applications DEXA'98. 1998. Vienna, Austria.: IEEE Computer Society.

[16] Kirkgöze, R., et al. A Security Concept for OLAP. In 8th Int. Workshop on Database and Expert System Applications DEXA'97. 1997. Toulouse, France: IEEE Computer Society.

[17] Lodderstedt, T., D. Basin, and J. Doser. SecureUML: A UML-based modeling language for model-driven security. In UML 2002. 2002. Germany: Springer.

[18] Mahboubi, H., M. Hachicha, and Darmont, J. XML warehousing and OLAP. Encyclopedia of Data Warehousing and Mining, 2nd Ed., IGI Publishing, pp 2109-2116, 2008.

[19] Mouratidis, H. and P. Giorgini, Integrating Security and Software Engineering: Advances and Future Vision. IGI Global. 2006.

[20] OMG. MDA Guide Version 1.0. Document number omg/2003-05-01. Ed.: Miller, J. and Mukerji, J. Retrieved from: http://www.omg.com/mda, 2003.

[21] OMG, Query/Views/Transformation RFP. 2002 Retrieved from: http://omg.org/ad/2002-4-10.

[22] Park, B.-K., H. Han, and I.-Y. Song, XML-OLAP: A Multidimensional Analysis Framework for XML Warehouses. Data Warehousing and Knowledge Discovery, 2005. LNCS 3589: p. 32-42.

[23] Pérez, J.M., Berlanga, R., Aramburu, M.J. and Bach Pedersen, T. Integrating Data Warehouses with Web Data: A Survey. IEEE Transaction Knowledge Data Engineering, 2008. 20(7): p. 940-955.

[24] Pérez, J.M., Berlanga, R., Aramburu, M.J. and Bach Pedersen, T.A relevance-extended multi-dimensional model for a data warehouse contextualized with documents. DOLAP 2005: p.19-28

[25] Priebe, T. and G. Pernul. A Pragmatic Approach to Conceptual Modeling of OLAP Security. In 20th Int. Conference on Conceptual Modeling (ER 2001). Yokohama, Japan: Springer-Verlag.

[26] Priebe, T. and G. Pernul. Towards OLAP Security Design - Survey and Research Issues. In DOLAP'00. 2000. Washington DC, USA.

[27] Rizzi, S., Abelló, A., Lechtenbörger, J. and Trujillo, J. Research in data warehouse modeling and design: dead or alive? DOLAP, p.3-10, 2006.

[28] Rosenthal, A. and Sciore, E. View Security as the Basic for Data Warehouse Security. 2nd Int. Workshop on Design and Management of Data Warehouse (DMDW'00). 2000. Sweden.

[29] Rusu, L., W. Rahayu, and Taniar, D. A Methodology for Building XML Data Warehouses. IJDWM 1(2): 23-48. 2005.

[30] Sapia, C., Blaschka, M., Höfling, G. and Dinter, B. Extending the E/R Model for the Multidimensional Paradigm. In: 1st International Workshop on Data Warehouse and Data Mining (DWDM'98). LNCS-1552. Springer-Verlag, p. 105-116. 1998

[31] Thuraisingham, B., M. Kantarcioglu, and S. Iyer, Extended RBAC-based design and implementation for a secure data warehouse. Int. Journal of Business Intelligence and Data Mining (IJBIDM), 2007. 2(4): p. 367-382.

[32] Tryfona, N., F. Busborg, and Christiansen, J. starER: A Conceptual Model for Data Warehouse Design. In: ACM 2nd International Workshop on Data Warehousing and OLAP (DOLAP'99). 1999. Missouri, USA: ACM.

[33] Van de Riet, R. P. Twenty-five years of Mokum: For 25 years of data and knowledge engineering: Correctness by design in relation to MDE and correct protocols in cyberspace. Data & Knowledge Engineering, 2008. 67(2): p. 293-329.

[34] Vela, B. Fernandez-Medina, E., Marcos ,E. and Piattini, M. Model Driven Development of Secure XML Databases. Sigmod Record. ACM Press, 2006, Vol. 35, 3, pp. 22-27.

[35] W3C XML Schema Working Group. XML Schema Parts 0-2:[Primer, Structures, Datatypes]. W3C Recommendation. Retrieved from: http://www.w3.org/TR/xmlschema-0/, http://www.w3.org/TR/xmlschema-1/ and http://www.w3.org/TR/xmlschema-2/, 2004.

[36] Wang, L., S. Jajodia, and D. Wijesekera. Securing OLAP Data Cubes Against Privacy Breaches. in IEEE Symposium on Security and Privacy. 2004. Berkeley, California.

[37] Weippl, E., et al. An Authorization Model for Data Warehouses and OLAP. In: Workshop on Security in Distributed Data Warehousing. 2001. New Orleans, Louisiana, USA.

[38] Wiwatwattana, N., et al., X^3: A Cube Operator for XML OLAP, In ICDE 2007: Istanbul, Turkey. p. 916-925.