Proceedings

DEXA

ARES 2007

In Cooperation with

enisa European Network and Information Security Agency

TU WIEN Technische Universität Wien Vienna University of Technology

[SECURE] Business Austria

Oesterreichische Computer Gesellschaft Austrian Computer Society

IEEE Computer Society Conference Publications Operations Committee

CPOC Chair

Phillip Laplante
Professor, Penn State University

Board Members

Mike Hinchey, *Director, Software Engineering Lab, NASA Goddard*
Linda Shafer, *Professor Emeritus, University of Texas at Austin*
Jeffrey Voas, *Director, Systems Assurance Technologies, SAIC*
Thomas Baldwin, *Manager, Conference Publishing Services* (CPS)

IEEE Computer Society Executive Staff

David Hennage, *Executive Director*
Angela Burgess, *Publisher*

IEEE Computer Society Publications

The world-renowned IEEE Computer Society publishes, promotes, and distributes a wide variety of authoritative computer science and engineering texts. These books are available from most retail outlets. Visit the CS Store at *http://www.computer.org/portal/site/store/index.jsp* for a list of products.

IEEE Computer Society *Conference Publishing Services* (CPS)

The IEEE Computer Society produces conference publications for more than 200 acclaimed international conferences each year in a variety of formats, including books, CD-ROMs, USB Drives, and on-line publications. For information about the IEEE Computer Society's *Conference Publishing Services* (CPS), please e-mail: tbaldwin@computer or telephone +1-714-821-8380. Fax +1-714-761-1784. Additional information about the IEEE Computer Society's *Conference Publishing Services* (CPS) can be accessed from our web site at: *http://www.computer.org/cps.*

IEEE Computer Society / Wiley Partnership

The IEEE Computer Society and Wiley partnership allows the CS Press *Authored Book* program to produce a number of exciting new titles in areas of computer science and engineering with a special focus on software engineering. IEEE Computer Society members continue to receive a 15% discount on these titles when purchased through Wiley or at: *http://wiley.com/ieeecs*. To submit questions about the program or send proposals, please e-mail: dplummer@computer.org or telephone +1-714-821-8380. Additional information regarding the Computer Society's authored book program can also be accessed from our web site at: *http://www.computer.org/portal/pages/ieeecs/publications/books/about.html.*

Revised: 17 August 2006

New *CPS Online* Workspace

An IEEE Online Collaborative Publishing Environment

We're proud to announce the launch of ***CPS Online***, a new IEEE online collaborative conference publishing environment designed to speed the delivery of price quotations and provide conferences with anytime access to all of a project's publication materials during production, including the final papers. **CPS Online**'s workspace gives a conference the opportunity to upload files through any Web browser, check status and scheduling on a project, make changes to the Table of Contents and Front Matter, approve editorial changes and proofs, and communicate with a CPS editor through discussion forums, chat tools, commenting tools and e-mail.

The following is the URL link to the CPS Online Publishing Inquiry Form:
http://www.ieeeconfpublishing.org/cpir/inquiry/cps_inquiry.html

Published by the IEEE Computer Society
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314

IEEE Computer Society Order Number P2775
Library of Congress Number 2007922437
ISBN 0-7695-2775-2

The Second International Conference on Availability, Reliability and Security

DEXA

ARES 2007

10 - 13 April 2007

Vienna, Austria

In Cooperation with

enisa European Network and Information Security Agency

TU WIEN Technische Universität Wien Vienna University of Technology

[SECURE] Business Austria

Österreichische Computer Gesellschaft Austrian Computer Society

IEEE Computer Society

IEEE

Los Alamitos, California

Washington • Tokyo

CPS Conference Publishing Services

IEEE Computer Society Order Number P2775
ISBN 0-7695-2775-2
ISBN 978-0-7695-2775-8
Library of Congress Number 2007922437

Additional copies may be ordered from:

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1 800 272 6657
Fax: + 1 714 821 4641
http://computer.org/cspress
csbooks@computer.org

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1 732 981 0060
Fax: + 1 732 981 9667
http://shop.ieee.org/store/
customer-service@ieee.org

IEEE Computer Society
Asia/Pacific Office
Watanabe Bldg., 1-4-2
Minami-Aoyama
Minato-ku, Tokyo 107-0062
JAPAN
Tel: + 81 3 3408 3118
Fax: + 81 3 3408 3553
tokyo.ofc@computer.org

Individual paper REPRINTS may be ordered at: <reprints@computer.org>

Editorial production by Bob Werner
Cover art production by Joe Daigle/Studio Productions
Printed in the United States of America by The Printing House

Conference Publishing Services
http://www.computer.org/proceedings/

Table of Contents

Second International Conference on Availability, Reliability and Security (ARES 2007)

Session 1: Trust Model & Trust Management

Session 2: Availability, Fault-Tolerant & Recovery

Session 3: Reputation Management & Trust

Session 4: Privacy & Access Control

Session 5: Failure Detection & Attack Prevention

Session 6: Authentication & Authorisation

Session 7: Security Algorithm & Framework

Session 8: Software Security

Session 9: Security Models

Session 10: Miscellaneous Security Techniques

Session 11: eAuction & eVoting Protocol

Session 12: Dependability in Distributed & Ubiquitous Computing

Session 13: Anomaly & Intrusion Detection

International Symposium on Frontiers in Availability, Reliability and Security (FARES)

Session 1: Fault-Tolerant & Availability

Session 2: Access Control

Session 3: Authentication

Session 4: Real-Time System & Sensor Network

Session 5: RFID Techniques & Applications

Session 6: Secure Solution & Applications

Session 7: Security Issue in Business Management

Session 8: Web, XML, Content Management

Session 9: Security Policies & Techniques

Session 10: Trust Management & Trust Model

Session 11: Miscellaneous Applications

Second International Workshop Dependability Aspects on Data Warehousing and Mining Applications (DAWAM 2007)

2nd International Workshop Dependability and Security in e-Government (DeSeGov 2007)

Workshop on Foundations of Fault-tolerant Distributed Computing (FOFDC 2007)

First International Workshop on Secure Software Engineering (SecSE 2007)

Workshop on "Modeling, Designing, and Testing Correct, Secure, and Dependable Event-Based System" (EBITS 2007)

First International Workshop on Advances in Information Security (WAIS 2007)

Workshop on "Security in E-Learning" (SEL)

Message from the Organizing Committee

Security, Reliability and Availability of IT systems and infrastructures have for over two decades been core research areas in the field of IT Security. Recent strategic research foci, especially in the European Union, have renewed the interest in the area and are setting the stage for very interesting and challenging developments, in areas ranging from the use of IT for increasing security in general, to the security of critical IT infrastructures and legal, economic and social issues. That is why ARES 2007, like ARES 2006 before, is again designed to serve as a bridge and discussion forum for researchers and practitioners.

We are therefore very pleased to have this conference for a second time organised in cooperation with ENISA (The European Network and Information Security Agency). ENISA supports the idea of this conference due to the urgent need of scientific research and the dissemination of new techniques in these areas.

We hope that this years ARES conference will again have a significant benefit for innovative applications which have to consider the various dependability issues and furthermore will build a platform for in-depth discussions between researchers in the different areas of Dependability, such as Availability, Reliability, and Security.

We have received 212 competed, on time submitted papers amongst over 250 abstract submissions from 43 countries for ARES 2007 and the Program Committee eventually selected 59 papers, making an acceptance rate of 27,83 % of submitted papers.

Seven workshops are organised on special topics of ARES, i.e.-

- Workshop "Dependability Aspects on Data Warehousing and Mining applications" (DAWAM 2007)
- Workshop "Dependability and Security in e-Government" (DeSeGov 2007)
- Workshop "Foundations of Fault-tolerant Distributed Computing" (FOFDC 2007)
- Workshop "Secure Software Engineering" (SecSE 2007)
- Workshop "Modeling, Designing, and Testing Correct, Secure, and Dependable Event-Based System" (EBITS 2007).
- Workshop "Advances in Information Security" (WAIS 2007)
- Workshop: Security in E-Learning (SEL 2007)

As an additional feature of ARES we have invited distinguished scientists for the International Symposium on Frontiers in Availability, Reliability and Security (FARES) to present and discuss special aspects relevant for future applications and research. We would like to express our gratitude to all program committee members, workshop organisers and committee members and all the external referees who reviewed the papers very profoundly and in a timely manner. Due to the high number of submissions and the high quality of the submitted papers, the reviewing, and discussion process was an extraordinarily challenging task.

Special thanks must be given to Dr. Tho Manh Nguyen for all his essential support in the organization of the PC-tasks of ARES 2007. We would also like to thank all the authors who submitted their papers to *ARES 2007* as their contributions built the basis of this year's excellent technical program. Many thanks go to Ms. Gabriela Wagner for her invaluable support with administrative issues.

Norman Revell, *Middlesex University, United Kingdom*

Roland Wagner, *University of Linz, Austria*

Honorary Co-Chairs

Günther Pernul, *University of Regensburg, Germany*

Makoto Takizawa, *Tokyo Denki University, Japan*

General Co-Chairs

Gerald Quirchmayr, *University of Southern Australia, Australia*

A Min Tjoa, *Vienna University of Technology, Austria*

Program Co-Chairs

pplication of QVT for the Development of Secure Data Warehouses: A case study

Emilio Soler[1], Juan Trujillo[2], Eduardo Fernández-Medina[3] and Mario Piattini[3]
(1) Departamento de Informática. University of Matanzas, Cuba
Autopista de Varadero km 3. Matanzas, Cuba.
emilio.soler@umcc.cu, http://www.umcc.cu
(2) Departamento de Lenguajes y Sistemas Informáticos. University of Alicante, Spain
C/ San Vicente S/N 03690 Alicante, Spain
jtrujillo@dlsi.ua.es, http://www.dlsi.ua.es
(3) Grupo ALARCOS, Departamento de Tecnologías y Sistemas de Información
Centro Mixto de Investigación y Desarrollo de Software UCLM-Soluziona
University of Castilla-La Mancha
Paseo de la Universidad, 4 – 13071 Ciudad Real, Spain
{eduardo.fdezmedina, mario.piattini}@uclm.es}, http://www.uclm.es

Abstract

t a crucial aspect for the development of rehouses (DW) because they contain sensitive ion. The application of the Model Driven ure (MDA) in the secure modeling of DWs btaining the secure logical scheme from the al model. In this paper, we apply the ViewTransformations (QVT) language to the ment of a secure DW by means of a case study. e introduce the case study related to a typical system. Afterwards, with the application of a QVT relations, we transform all the captured and audit requirements from the ensional conceptual model of the DW, to the level, by means of the construction of a e model. From this scheme it turns out easier n code for a specific platform that implements and audit aspects.

oduction

dimensional modeling (MD) is the n of Data Warehouses (DWs). MD and On-Line Analytical Processing applications. These applications are used in ion to form a highly powerful mechanism owering crucial business information in decision-making processes.

ses store historical information which is d from multiple, heterogeneous, autonomous ibuted data sources, thereby, the survival of the organizations depends on the correct management, security and confidentiality of the information [1]. The information security is a serious requirement which must be given careful thought to, not as an isolated aspect, but as an present element in all stages of the lifecycle development, from requirement analysis to implementation and maintenance [2]. Therefore, it is crucial to specify confidentiality measures in the MD modelling process, and to enforce them.

The Unified Modeling Language (UML) profile presented in [3] allows us to specify the main aspects of security in a MD model. In [4] we present an extension of the relational package of the Common Warehouse Metamodel (CWM) that allow us to specify at the logical level all the considered security and audit measures in the conceptual modeling of DWs. These two proposals are integrated under the Model Driven Architecture (MDA) framework [5], to establish a secure platform independent model (secure PIM) and a secure platform specific model (secure PSM), as well as a set of Query/View/Transformations (QVT) relations for the modeling of secure DWs. Hereby we propose a solution to the semantic gap between advanced conceptual data models and relational or multidimensional implementations of data cubes [6].

In this work we apply a set of QVT relations to the development of a secure DW. The case study presented is related to a sanitary typical system. The considered multidimensional conceptual model is transformed into a relational logical scheme and from this we explain how to obtain code for a target platform. To this aim, we use a secure multidimensional PIM (SMD PIM)

and a secure multidimensional PSM (SMD PSM) as well as the relations defined in [5].

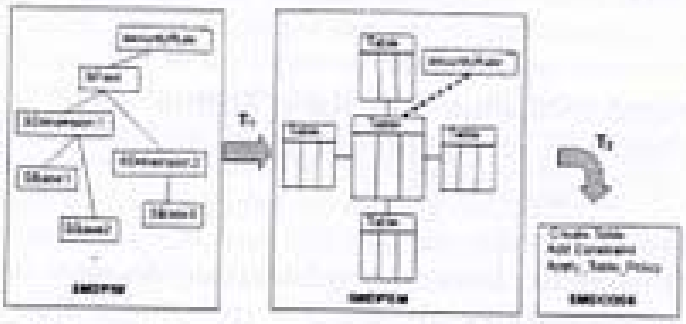


Figure 1. General transformation scheme

The diagram in Figure 1 illustrates a reduced approximation of the Secure Multidimensional MDA architecture [5]. On the left hand side the Secure Multidimensional conceptual scheme, i.e., SMD PIM, is presented. By means of the transformation T_1 we obtain the relational logical scheme, i.e., SMD PSM, represented in the centre of Figure 1. If we choose a SGBD that implements security aspects, then SMD PSM is transformed according to T_2 into code for the target platform. This code is called the Secure Multidimensional Code (SMD Code). The Figure illustrates how the security constraint defined by means of a securityRule [3, 4] (represented as an UML note) is transformed from the conceptual level to the logical level by employing T_1, and later transformed into code with the T_2 transformation.

The rest of this paper is structured as follows. Section 2 begins introducing the case of study related to a typical sanitary system. It follows an explanation of the conceptual multidimensional modeling to introduce the secure PIM, this section finishes with the application of the QVT transformations to obtain the secure PSM. Finally, section 3 draws the main conclusions and outlines our immediate future work.

2. Case study

In this section, we apply the QVT transformations to the development of a secure DW related to a typical sanitary system. We have omitted some details to make the case of study more understandable. The example is an extended version of [4].

2.1 Introduction to the case study

A hospital desires to automate the incomes of the patients as well as to keep million of complex records treatments realized to patients. A sanitary system manipulates highly confidential information, so it is mandatory to build a DW that contemplate a
way security requirements (see Figure 2)

The Admission class keeps information
patients that enter to one or more hospitals.
the data of the patient and its diagnosis are
the classes, Diagnosis, Patient, Time, Diagnos
and City. The class UserProfile contains
all the users that will have access to the
order to store the information of the patient
diagnosis are necessary the Diagnosis, Patient,
Diagnosis_Group and City classes. The
class contains information of all the users
have access to the system.

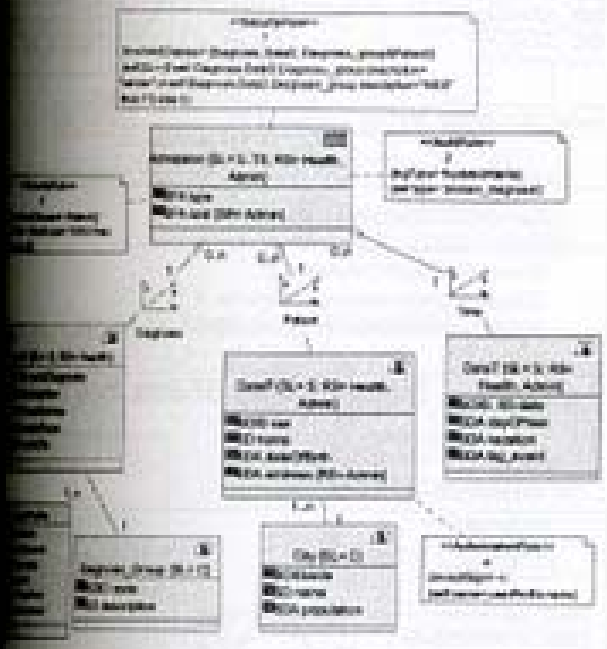
We have used the following security
confidential, secret and topSecret. User roles
Health (including Doctor and Nurse subroles)
nonHealth (including Maintenance and
subroles) have been defined. The root
hierarchical roles tree is HospitalEmployer.
example we have not considered
compartments.

2.2 Conceptual multidimensional modeling

Figure 2 shows a secure MD model that
fact class (Admission), three dimensions
(Diagnosis, Patient and Time), five base
(DataD, Diagnosis_Group, DataP, City,
and a UserProfile class. The Admission fact
SFact stereotype- contains all the
admissions of patients in one or more hospitals
can be acceded by all the users who have
levels secret or topSecret -labeled value
(SL)-, and perform health or administrative
tagged value SecurityRoles (SR)-. Be
the attribute cost only can be acceded by
play administratively role - tagged value SR-
base DataP contains the information of the
the hospital and can be acceded by all the
have security level secret - tagged value SL-,
health or administrative roles -t value SR-.

The Address attribute can be only accessed by
who have an administrative role -tagged value
attributes-. City base class contains the
cities, and it allows us to group patients by
base class can be accessed by all users who
confidential security level -tagged value SL-.
base contains the information of each user
and can be accessed by users who have a
tagged value SR-, and have secret security
tagged value SL-. Finally Diagnosis_group
set of general groups of diagnosis. Each group
related to several diagnoses, but a diagnosis
always related to a group. Diagnosis_group
accessed by all users who have confidential

-tagged value SL-. Some security constraints been specified by using the previously defined straints, stereotypes and tagged values:



ure 2. Example of secure multidimensional modeling

The security level of each instance of Admission defined by a security constraint specified in the model. If the value of the SDescription attribute of the Diagnosis_group to which diagnosis belongs is cancer or AIDS, the security level - tagged value SL- of this admission will be top secret, otherwise secret. This constraint is only applied if the user makes a query whose information comes from Diagnosis dimension or Diagnosis_group base classes, together with DataP base -tagged value involvedClasses-. Therefore, a user who has secret security level could obtain the number of patients with cancer for each city, but never its information of DataP base appears in the query.

The tagged value logType has been defined for Admission class, specifying the value frustratedAttempts. This stereotype specifies that the system has to record, for future audit, the situation in which a user tries to access information whose type is 'primary diagnosis' of the fact class, and so where the system denies it because of lack of permission.

The security level –tagged value SL- of each instance of Admission can also depend on the value of cost attribute, which indicates the price of the admission service. In this case, the constraint is only applicable to queries that contain information of the DataP base -tagged value involvedClasses-.

4. Patient could be special users of the system. In this case, it could be possible that patients access their own information as patients (for instance, for querying their personal data). This constraint is specified by using the exceptSign tagged value in the DataP class.

The privilege that is considered in these exception is read, but we have not specified it in the model (the default value of exceptPrivilege tagged value is Read).

In Figure 2 we have represented an instance of the PIM, that we have been called Secure Multidimensional PIM (SMD PIM) [5]. In this model the Admission class represents a SFact, whereas Diagnosis, Patient and Time represent SDimension classes. In this example we do not consider SDegenerateFact. Diagnosis_Group and City represent SBase classes. In these classes we can model security requirements, for that reason, by means of notes of UML [7] we represent the AuditRule, AuthorizationRule and SecurityRule classes, in this way we establish security rules in the multidimensional conceptual model. At the attribute level the security is established by means of the SFactAttribute, SOID, SDescriptor and SDimensionAttribute classes.

2.3 QVT relations to obtain the PSM

A platform specific model (PSM) is a system view from the perspective of the platform. A PSM combines the specification of the PIM with the details that specify how the system uses a certain type of platform [8]. In the design of databases and data warehouses, the conceptual modeling provides the PIM, and the logical modeling the PSM. In multidimensional modeling, the logical level is designed according to the specific properties of the SGBD (Relational Online Analytical Processing, ROLAP, Multidimensional Online Analytical Processing, MOLAP or Hybrid Online Analytical Processing, HOLAP). Still, Kimball [9] assures that the most common representation is on relational platforms, i.e., on ROLAP systems.

The SMD PSM allows us to represent at the relational level the security requirements that were represented in the conceptual modeling of the DW. In this model we can represent tables, columns, primary and foreign keys, etc. Thus, we can establish security in attributes and tables. By means of UML notes [7] we express the security constraints that were modelled at the conceptual level.

In order to establish the transformation between SMD PIM and SMD PSM we consider the QVT declarative approach [10].

The main transformation contains relations of the type top-level. In each relation, we specify pre and post-conditions that should satisfy the relation by means of the clauses *when* and *where*. In Figure 3 we have represented the main transformation. The first relation in executing is SecureDW2SSchema, with it, all levels of security: confidential, secret and topsecret, as well as all the hierarchical roles tree is transformed into their equivalent ones of SSchema. The UserProfile2RUserProfile relation transforms the UserProfile class into a table belonging to SSchema that will have the same name of UserProfile. The relation that follows, i.e., SFact2STable is shown in its graphical notation in Figure 4, by means of this relation each SFact jointly with its security properties is transformed into a table that will contain the same information of security.

```
Transformation SMD To SREL(SMD: SECDW)
    SREL: SECRDW)
{
key Table(name, Schema);
key Column (name, owner);
key UserProfile(name, Schema);
key PrimaryKey(name, owner);
key ForeignKey(name, owner);
key SecurityProperty(name, owner);
key SecurityConstraint(name, owner);
top relation SecureDW2SSchema();
top relation UserProfile2RUserProfile()
top relation SFact2TAble ()
top relation SDegenerateFact2STable()
top relation SDimension2STable()
  //Association SFact with SDimension
top relation AssocSF_SD2FKey()
  //Association SDegenerateFact with SDimension
top relation Assoc SDF_SD2FKey
// Association SDegenerateFact with SFact
top relation AssocSDF_SF2FKey()
}
```

Figure 3. SMD PIM to SMD PSM transformation

The clause *where* invokes to the relations that must be executed. In Figure 5, we are going to show how the attributes of SFact are transformed into SColumns of the table that represents the SFact, so that, each column will contain the security information of its corresponding attribute in the SFact.

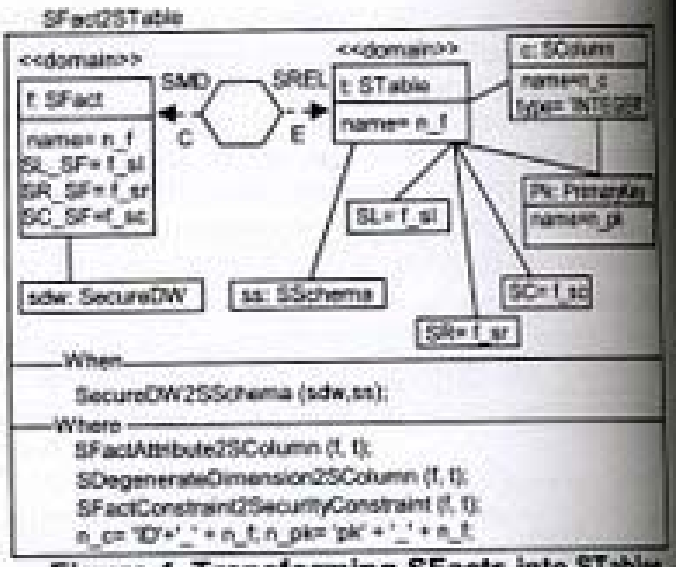


Figure 4. Transforming SFacts into STables

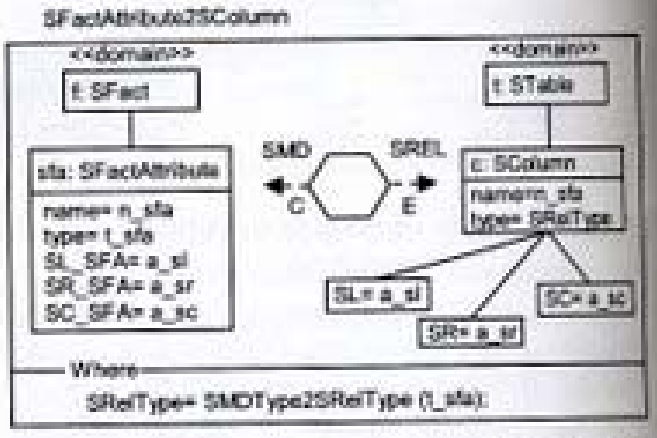


Figure 5. Transforming SAttributes into SColumns

In Figure 6 we show the result of applying the SFact2STable relation to our case study. The SFact Admission is transformed into a table of the model SMD PSM, i.e., in the Admission table, that will have a primary key, as well as the security properties securityLevel and securityRole.

Figure 7 shows the result of applying the SFactAttribute2SColumn relation, as a consequence, the Admission table will contain the columns respectively type and cost of type string and float. The column cost will have associated the security property securityRole. Also in Figure 7, the associated requirements of security to the Admission table are modeled in the heading of the table, according to the SECRDW metamodel[4].

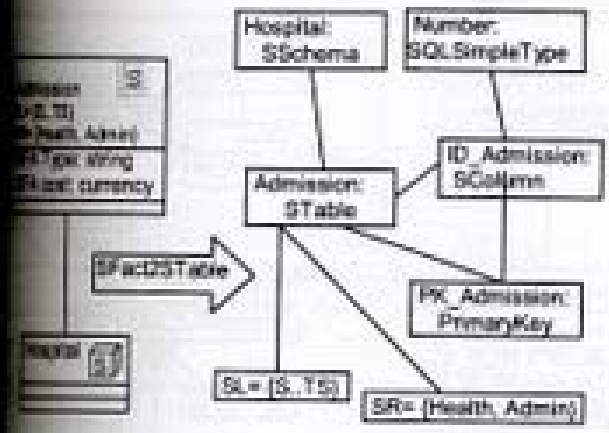


Figure 6. Applying SFact2STable

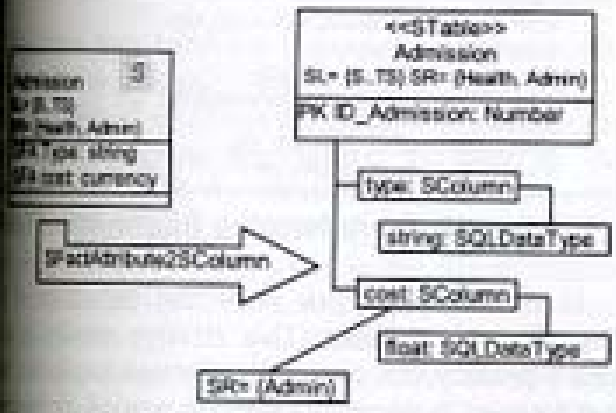


Figure 7. Applying SFactAttribute2SColumn

Next, the relations that appear in the clause *where* of SFact2STable must be executed. First the SDegenerateDimension2SColumn relation should be applied, but in our case we don't have many-to-many relationship between the SFact Admission and the dimensions. For that reason we will not define this relation.

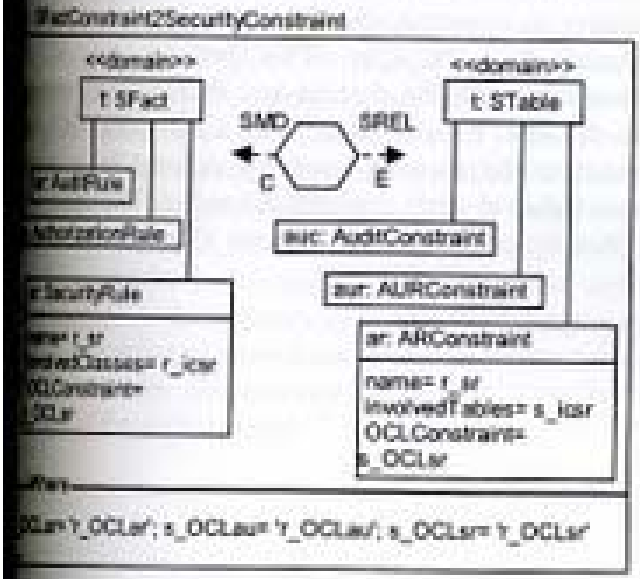


Figure 8. SFactConstraint2SecurityConstraint

Figure 8 presents the definition of the SFactConstraint2SecurityConstraint relation, which guarantees that all the constraints associated with the SFact are transformed in constraints associated with the table, just as it can be seen in Figure 9. The SECRDW metamodel [4], assures that these constraints are modelled at the logical level by means of notes associated with table.

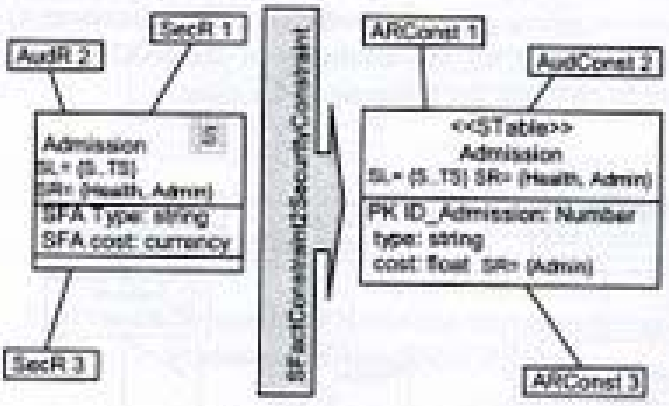


Figure 9. Applying SFactConstraint2SecurityConstraint

Continuing with the main transformation that appears in the Figure 3, it now corresponds to apply the SDegenerateFact2STable relation, which does not appear because all the relations between the SFact Admission and the dimensions are many-to-one. In Figure 10 we show the definition of the SDimension2STable relation.

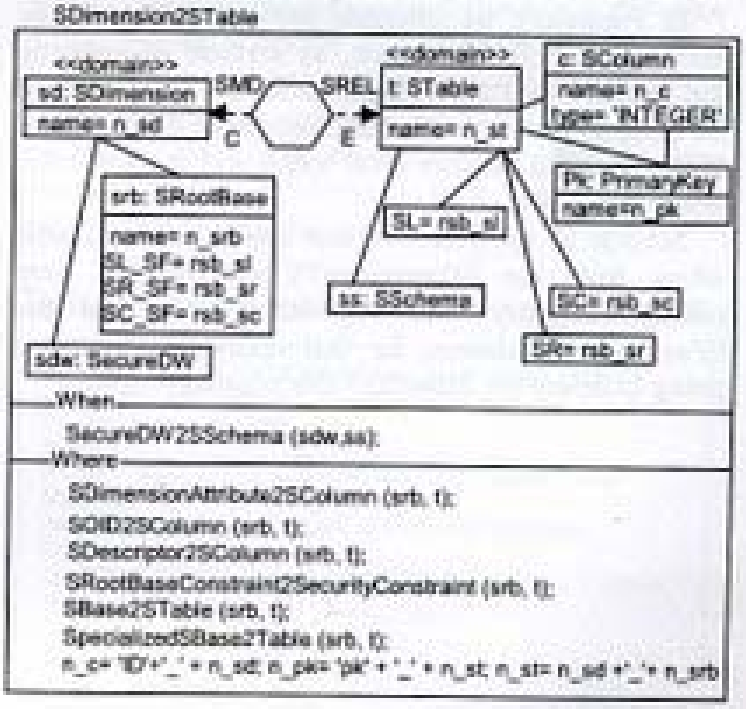


Figure 10. Transforming SDimension into STable

In multidimensional modeling the dimensions do not have attributes [10], for this reason, when the SDimension2STable relation is executed, a table is created whose name is merged with the names from dimension and rootBase respectively. The rootBase is the only SBase associated with the SDimension. All the associated security information with the rootBase is transformed in security properties of the table and by means of the execution of the relations that appear in the clause *where* of the SDimension2STable relation, is guaranteed that all the attributes of the rootBase are going to conform the columns of the table.

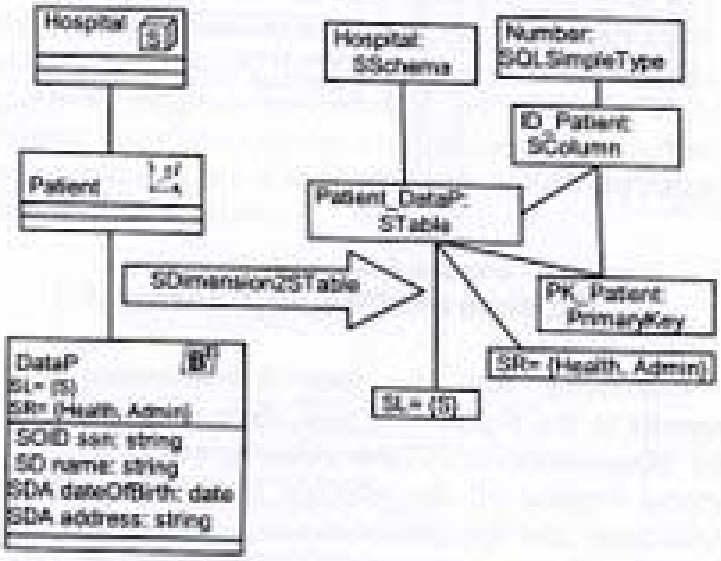


Figure 11. Applying SDimension2STable

In Figure 11 we illustrate the application of the SDimension2STable relation, as a result of applying this relation, the Patient_DataP table is created, with all the security properties that has associated the rootBase, in this case the security level secret and the user roles health and admin.

Several of the relations that appear in the clause *where* from the SDimension2STable relation keep certain similarity with the defined ones for the SFact2STable relation, for that reason; next we are going to define the SBase2STable relation

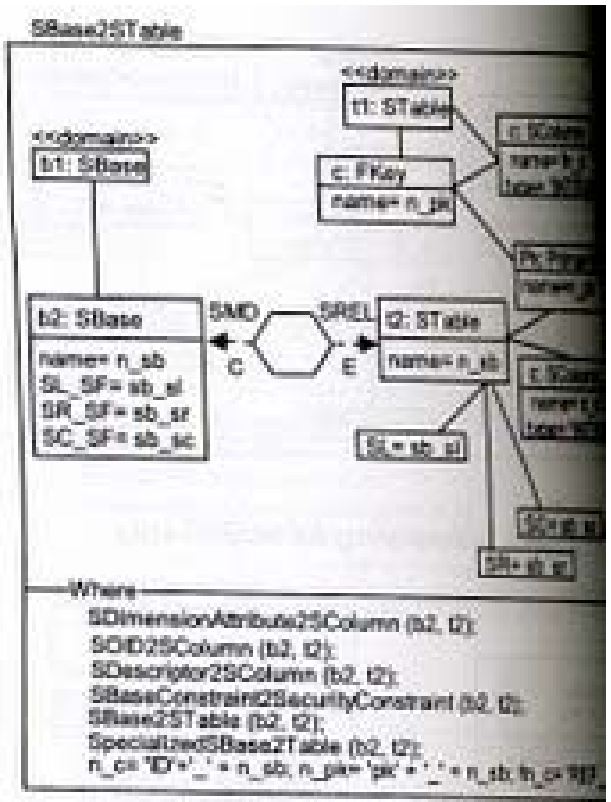


Figure 12. Transforming SBase into S

In the Figure 12 we show the definition SBase2STable relation. This relation creates with a primary key, as well as a foreign key in t that receives as parameter when it is invoked; l the primary key and the foreign key will be u for guaranteeing that the tables form a part of a one-to-many between the SBases. In the claus this relation is called again, as well SpecializedSBase2STable relation to assure us cover the whole hierarchy of bases that confo dimension.

In Figure 13 we illustrate the application SBase2STable relation to our case study. W relation is executed, the City table is created primary key PK_City. This primary key associated with the foreign key that is also c the STable Patient_Data. The City table w associate the security property defined by securityLevel with confidential value. The fi is that the tables City and Patient_DataP are re

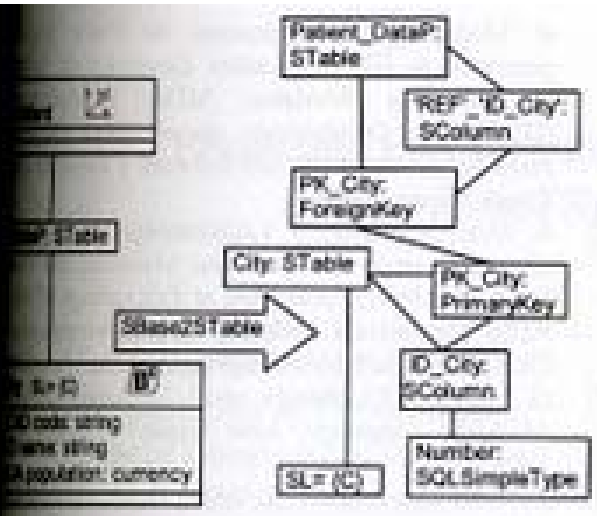


Figure 13. Applying SBase2STable

The first four relations that appears in the clause ...w of the SBase2STable relation guarantee the ...rmation of all SBase attributes in columns of the ... that represents the SBase, as well as the ...rmation of all the constraints associated to the ... is constraints associated to the table that ...sents the SBase. The calls to the SBase2STable ...SpecializedBase2STable relations permit to cover ...ively through all the hierarchy of bases that ...rms the dimension. The SpecializedBase2STable ...on has certain similarity with the SBase2STable ...ion, for that reason we are not going to define it.

...o complete the case study only remains apply the ...ocSF_SD2FKey, AssocSDF_SD2FKey and ...ocSDF_SF2FKey relations, which enable to ...blish relationships between SFact and the ...nsions, between the SDegenerateFact and the ...nsions and between the SFact and the ...generateFact. In our case only proceeds to ...blish relations between the SFact Admission and ... SDimensions, therefore we do not have ...generateFact. As consequence, when the ...ocSF_SD2FKey relation is applied, then three ...gn keys are created in the Admission table. These ... enable the relationships between the Admission ... with the Diagnosis_DateP, Patient_DataP and ...t_DataT tables.

...Figure 14 we have omitted the attributes in some ...s, as well as the primary keys and the foreign key ...ake the scheme snowflake more understandable. ...bserved how the security constraints have been ...lled at the logical level.

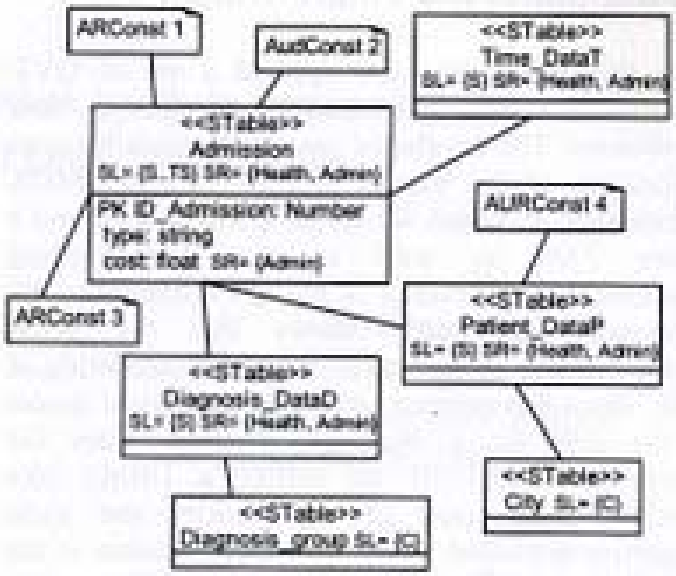


Figure 14 Snowflake schema representing a instance of the SMD PSM

In order to obtain code for a specific platform we choose Oracle 9i DBMS which allows us to implement multilevel databases and has a component named Oracle9i Label Security (OLS) [11]. OLS allows us to specify labeling functions and predicates that are triggered when an operation is executed, and which define the value of security labels according to a condition. To illustrate the possibilities of OLS we will only focus on the ARConstraint labeled with label number 3 in Figure 14. Table 1 (1) shows how by means of the creation of a function and the use of security labels we can define the following: if the value of Cost column is greater than 10000 then the security label will be composed of TopSecret security level and Health and Admin user roles, else the security label will be composed of Secret security level and the same user roles. Table 1 (2) shows how to link this labeling function with Admission table.

Table 1. Implementing security aspect in OSL

```
(1) CREATE FUNCTION Which_Cost (Cost: Integer) Return
LBACSYS.LABC_LABEL
As MyLabel varchar2(80)
Begin
If Cost > 10000 then MyLabel:= ' TS::Health, Admin'; else
MyLabel:= ' S::Health, Admin'; end if;
Return TO_LBAC_DATA_LABEL('MyPolicy', MyLabel);
End;
(2) APPLY_TABLE_POLICY ('MyPolicy', 'Admission', 'Scheme',
'Which_Cost')
```

3. Conclusions and Future Work

In this paper we have applied a set of QVT relations to the development of secure data warehouses. The developed case study constitutes an application of the Secure Multidimensional MDA architecture, in which we define a secure PIM and a secure PSM as well as the corresponding transformation by means of the QVT standard. The developed case study shows that the MDA framework can be applied to the secure modeling of DWs, since this permits to obtain the logical model of the DW for a relational platform from the conceptual model. If we utilize a DBMS like Oracle9i, then many of the security and audit properties modelled in the snowflake schema at the logical level can be transformed into code, in this way, we show that is possible to automate all the design process of secure DWs, which turns out to be a saving of time for the developers.

Our immediate future work consists of studying the possibility of implementing the QVT relations by using the capacity that offers some case tools.

Acknowledgements

This work has been partially supported by the METASIGN project (TIN2004-00779) from the Spanish Ministry of Education and Science, by the DADASMECA project (GV05/220) from the Regional Government of Valencia, and by the DIMENSIONS (PBC-05-012-1) DADS project (PBC-05-012-2) from the Regional Science and Technology Ministry of Castilla -La Mancha (Spain).

References

[1] G. Dhillon and J. Backhouse, "Information Systems Security Management in the New Millenium.," *Communications of the ACM*, vol. 43 (7), 2000.

[2] P. Devanbu and S. Stubblebine, "Software Engineering for Security: a Roadmap," presented at The Future of Software Engineering, Limerick, Ireland, 2000.

[3] R. Villarroel, E. Fernández-Medina, and M. Piattini, "A UML 2.0/OCL Extension for Designing Secure Data Warehouses," *Journal of Research and Practice in Information Technology*, vol. 38, 2006.

[4] E. Soler, R. Villarroel, J. Trujillo, E. Fernández-Medina, and M. Piattini, "Representing Security and Audit Rules for Data Warehouses at the Logical Level by using the Common Warehouse Metamodel," presented at First International Conference on Availability, Reliability and Security (ARES'06), Vienna, Austria, 2006.

[5] E. Soler, J. Trujillo, E. Fernández-Medina, and M. Piattini, "Un Conjunto de Transformaciones QVT para el Modelado De Almacenes de Datos Seg... presented at III Taller sobre Desarrollo de Soft... Dirigido por Modelos. MDA y Aplica... (DSDM'06). Desarrollado en el marco de las ... Jornadas de Ingeniería del Software y Bases de D... Sitges, España, 2006.

[6] S. Rizzi, A. Abelló, J. Lechtenbörger, and J. Trujillo, "Research in Data Warehouse Modeling and Design: Dead or Alive?," presented at Proceedings of the 9th ACM international workshop on Data warehousing and OLAP (DOLAP'06), Arlington, Virginia, USA, 2006.

[7] G. Booch, J. Rumbaugh, and I. Jacobson, *The Unified Modeling Language: User Guide*: Addison-Wesley, 1999.

[8] J. Miller and J. Mukerji, "MDA Guide Version 1.0.1," 2003.

[9] R. Kimball and M. Ross, *The Data Warehouse Toolkit*, 2 edition ed: John Wiley, 2002.

[10] QVT, "OMG 2nd Revised Submission: MOF 2.0 Query/Views/Transformations.," 2006.

[11] J. Levinger, " Oracle Label Security. Administrator's guide. Release 2.0 (9,.2)," 2002.