Towards Comprehensive Requirement Analysis for Data Warehouses: Considering Security Requirements

Emilio Soler[*], Veronika Stefanov[†], Jose-Norberto Mazón[‡],
Juan Trujillo[‡], Eduardo Fernández-Medina[§] and Mario Piattini[§]
[*]Departamento de Informática
Universidad de Matanzas, Cuba
Email: emilio.soler@umcc.cu
[†]Women's Postgraduate College for Internet Technologies
Institute of Software Technology and Interactive Systems
Vienna University of Technology, Austria
Email: stefanov@wit.tuwien.ac.at
[‡]Departamento de Lenguajes y Sistemas Informáticos
Universidad of Alicante, Spain
Email: {jnmazon,jtrujillo}@dlsi.ua.es
[§]Departamento de Tecnologías y Sistemas de Información
Universidad de Castilla-La Mancha, Spain
{Eduardo.FdezMedina,Mario.Piattini}@uclm.es

***Abstract*—Data warehouse (DW) systems integrate data from heterogeneous sources and are used by decision makers to analyze the status and the development of an organization. Traditionally, requirement analysis approaches for DWs have focused purely on information needs of decision makers, without considering other kinds of requirements such as security or performance. But modeling these issues in the early stages of the development is a cornerstone for building a DW that satisfies user expectations. In this paper, we define the two kinds of requirements for data warehousing as *information* and *quality-of-service* requirements and combine them in a comprehensive approach based on MDA (Model Driven Architecture). This allows a separation of concerns to model requirements without losing the connection between information and quality-of-service, also in the following conceptual or logical design stages. Finally, in this paper, we introduce a security requirement model for data warehousing, and a three-step process for modeling security requirements, thus illustrating the applicability of our approach with an example.**

I. Introduction

Data Warehouse (DW) systems are used by decision makers to analyze the status and the development of an organization [8], based on large amounts of data integrated from heterogeneous sources into a multidimensional (MD) model. Measures such as the number of transactions per customer or the increase of sales during a promotion are used to recognize trends or warning signs and to decide on future investments.

MD models are special conceptual data models which allow data access in a way that comes more natural to human analysts. The data is located in n-dimensional space, with the dimensions representing the different ways the data can be viewed and sorted (e.g., according to time, store, customer, product, etc.). Designers of MD models have to structure the information that is available into facts and dimensions. Facts are usually measures of business processes of some kind (e.g., how many products are sold, how many patients treated, how long something takes, etc.), and dimensions represent the context for analyzing these measures.

In data warehousing today, requirements approaches have a strong focus on the data model [17]. As input for the conceptual model, the schemata of the available operational data sources are compared with the information requirements of the users [7], [13], [23]. The problem is that the final product of the DW design process is not just a data model but a whole DW system, where users require that the information has some characteristics when it is provided (security, performance tuning, user configurations, etc.). These characteristics are constraints that the DW must fulfil to satisfy user expectations. We have named them quality-of-service (QoS) requirements, because they are additional issues that must be fulfilled by the DW to add quality in the way that the information is supplied and used. Informally speaking, information requirements answer *what* information the DW is expected to provide, and QoS requirements answer *how* this information should be provided for a right use.

The QoS requirements influence the data model and each other, and should be considered neither separate, nor added later. Even though they are external to the information requirements, QoS requirements are closely related to them. Therefore, we identify a need for an approach as shown in Figure 1, where QoS requirements can be considered

- together with information requirements, and
- from the early stages of the development onwards.

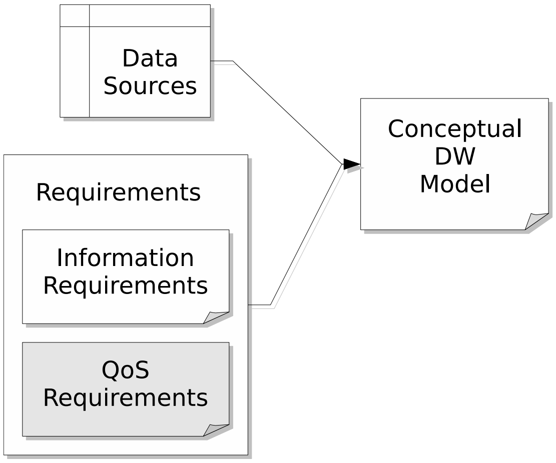


Fig. 1. QoS Requirements are needed as input for data warehouse design.

In this paper we present a comprehensive approach to requirement analysis for DW. We integrate QoS requirement analysis into an existing DW framework for information requirements [10]. In connection with the Model-Driven Architecture (MDA), this framework allows designer [12] to (i) derive database schemata and other parts of the final DW system, such as access control configuration files, and (ii) achieve separation of concerns without losing the connection between information requirements and QoS requirements, by modeling both in a CIM (Computation Independent Model, in the MDA framework).

QoS requirements include a lot of issues: how the data is presented in a correct visualization, how the data is made accessible in a secure way, how the data access is implemented to reach the desired performance, and so on. Because of the wide variety of QoS requirements and the limited length of this paper, we focus on one aspect only: *Security*. Our motivation is that, as some authors have remarked [2], [3], [6], security of information is a serious requirement which must be carefully considered, not as an isolated aspect, but as an element which turns up as an issue in all stages of the development lifecycle, from requirement analysis to implementation and maintenance. Therefore, DW designers must be provided with models specifying security aspects. Authentication, access control and audit jointly provide the foundation for information security [18]. Authentication[1] establishes the identity of one party to another. Access control determines what one party will allow another one to do with respect to resources and objects mediated by the former. Access control usually requires authentication as a prerequisite. The Audit process gathers data about activities in the system and analyzes it in order to discover security violations or to diagnose their cause. Therefore, in this paper, we consider security requirements as those related to access control and audit issues.

Section IV describes the details of how the security requirements can be derived and integrated with information requirements. We introduce a model for DW security requirements, and a three-step process for deriving them in a goal-oriented approach. This is illustrated with an example from the pharmaceutical domain.

Related work is treated in Section II, followed by our approach to modeling information and QoS requirements for DWs together in Section III. Section IV introduces the model for DW security requirements and gives an example. Section V concludes and presents open questions and future work.

II. Related Work

Only a few approaches have considered requirement analysis as a crucial task in early stages of the DW development. In [23], a method is proposed in order to both determine information requirements of DW users and match these requirements with the available data sources. The approach described in [16] introduces a requirement elicitation process for DWs by identifying the goals of the decision makers and the required information that supports the decision making process. Finally, in [7], the authors present a goal-oriented framework to model requirements for DWs, thus obtaining a conceptual MD model from them by using a set of guidelines.

However, these approaches only consider information requirements, i.e. interesting measures that the DW should store to support the decision making process and the context for their analysis. To the best of our knowledge, only the *data warehouse requirements definition* (DWARF) [14], [15] approach that adapts a traditional requirements engineering process for requirements definition and management of DWs, has considered the specification of other kind of requirements apart from information requirements, such as integrity, security or performance: non-functional requirements (similar to our QoS requirements) for DWs. The authors provide a classification of non-functional requirements that must be addressed in the development of DWs, and guidelines for their operationalization. Unfortunately, the specification of these requirements is considered in an isolated way, without taking information requirements into account. However, in order to obtain a conceptual MD model that drives the development of a DW which satisfies information needs and QoS expectations, both kind of requirements should be modeled together, since they are related. Therefore, we propose to perform requirements analysis for DWs as an essential stage of an overall approach for the development of DWs based on MDA, in which information and QoS requirements are modeled.

QoS is related to the concept of *usage*, as described by [22]. Usage models describe how a DW is being used, e.g., how often, by which user groups, how flexible the users' requirements are, how critical the availability of a certain DW service is, etc. Usage models can be derived from an existing DW and used to find potential improvements, or a new usage model can be designed for a DW to be built. The various aspects of usage are mirrored in QoS requirements. Both concepts try to capture not (only) *what* but *how* the DW is being used.

[1] Authentication is a mechanism that is design-independent and relies more on the company policies, and therefore, it is beyond the scope of this paper.

III. Requirement Analysis in Data Warehousing

The development of a DW is focused on the design of a conceptual MD model. As shown in Figure 1, the specification of this model must be driven by an analysis of (i) operational data sources, (ii) information requirements, and (iii) QoS requirements, in order to design a conceptual MD model that satisfies user expectations and agrees with the operational sources. In this paper, we focus on describing a comprehensive requirement analysis approach for DWs that comprises two main parts[2]:

1) **Information requirement analysis:** aims at obtaining information requirements of decision makers, i.e. interesting measures and the context for analyzing these measures. These information requirements must be specified in an information requirement model (see Sect. III-A).
2) **QoS requirement analysis:** enriches the information requirement model with QoS requirements to reflect under which constraints this information is delivered (see Sect. III-B).. The reason is that the information requirement model only reflects requirements for a "naked MD model" that only provides the right information to the users, while ignoring how this information is provided and used.

We have aligned this approach with an MDA framework for DWs [12]. In an MDA approach, requirements are specified in a highly abstract model, the CIM (Computation Independent Model). Once we have the specification of this CIM, we can derive a conceptual MD model, called Platform Independent Model (PIM) in MDA, that drives the implementation of the DW. Because this is out of the scope of this paper, we refer reader to [10], [12], [13] for further information on how DW implementations can be generated from these models.

A. Information requirement analysis

Decision makers who use DWs often ignore how to suitably describe information requirements, since they are rather concerned with the goals which the DW helps to fulfil. Therefore, a requirement analysis phase for DWs ideally starts discovering the goals of decision makers. The information requirements and the MD concepts can be discovered more easily from these goals.

Goals related to the DW can be specified on three levels [9]: *Strategic goals*, which are main objectives of the business process: "increase sales", "increase number of customers", "decrease cost", etc. *Decision goals* aim at taking the appropriate actions to fulfil a strategic goal, for example "define some kind of promotion" or "open new stores". Finally, *information goals* are related to the information required by a decision goal to be achieved; examples are "analyze customer purchases" or "examine stocks". Once these goals are defined, information requirements can be directly obtained from the information goals. The different MD elements, such as *facts* or *dimensions*, will be discovered from these information requirements in order to specify the corresponding conceptual MD model of the DW.

For modeling the information requirements, a UML profile for the *i** modeling framework [24] is used (see Figure 3). The *i** modeling framework provides mechanisms to represent different DW actors, their dependencies, and for structuring the business goals that the organization wants to achieve with the DW. Two models are used in i*: the *strategic dependency* (SD) model for describing the dependency relationships among various actors in an organizational context, and the *strategic rationale* (SR) model, used to describe actor interests and concerns, and how they might be addressed.

Information requirements for each actor (decision maker) are described in SR models. The SR model (modeled with the *SR* stereotype and represented as ◌) provides a detailed way of modeling internal intentional elements and relationships of each actor (*IActor*, ○).

In order to define SR models for DWs, goals (*Goal*, ⬭), tasks (*Task*, ⬡), and resources (*Resource*, ▭) are represented as intentional elements for each decision maker, as can be seen in Figure 2. These elements can be related via two kind of relationships: means-end (*MeansEnds*, —▷) or task-decomposition (*Decomposition*, —┼).

Our profile for i* has been extended in order to model requirements for the DW. Specifically, goals of decision makers can be defined by using the *Strategic*, *Decision*, and *Information* stereotypes by specializing the previously defined *Goal* stereotype. From information goals, information requirements (*Requirement*) are derived and represented as stereotyped tasks. Furthermore, requirement analysis for DWs needs some MD concepts to be added (in the sense of [7]). The following concepts are added as stereotyped resources: business processes related to the goals of decision makers (*BusinessProcess* stereotype), relevant measures related to information requirements of decision makers (*Measure*), and contexts needed for analyzing these measures (*Context*). The use of these elements can be seen in Figure 2. Additionally, foreseen relations between context of analysis are modeled. For instance, the *pharmacy* and the *pharmacy_type* contexts are related because pharmacies can be aggregated in types. For modeling these relationships, we use the (shared) aggregation relationship of UML (*Association* UML metaclass, represented as —◇). All of the described modeling elements are designed in our extended *i* profile* [10] (sketched in Fig. 3).

Goals and information requirements for the DW will be modeled and related to the required MD concepts in a CIM in several steps: (i) discovering the intentional actors (i.e. decision makers), thus defining SR models for each one, (ii) discovering the different kind of goals (iii) deriving information requirements from information goals, and (iv) obtaining the MD concepts related to the information requirements.

B. QoS requirement analysis

Once the information requirements have been specified in a CIM, the model is enriched by adding QoS requirements. QoS requirements are manifold. To not overlook any important

[2] The reader is referred to [11], [13] for a wider explanation about operational data sources analysis.

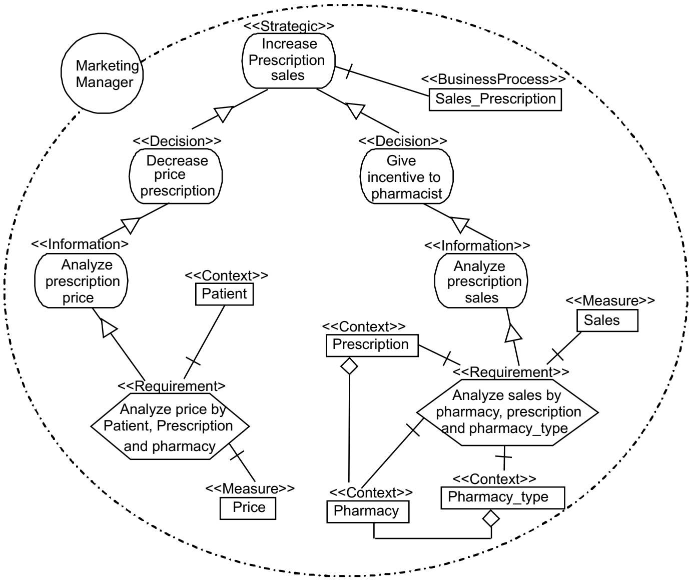


Fig. 2. Model of the information requirements.

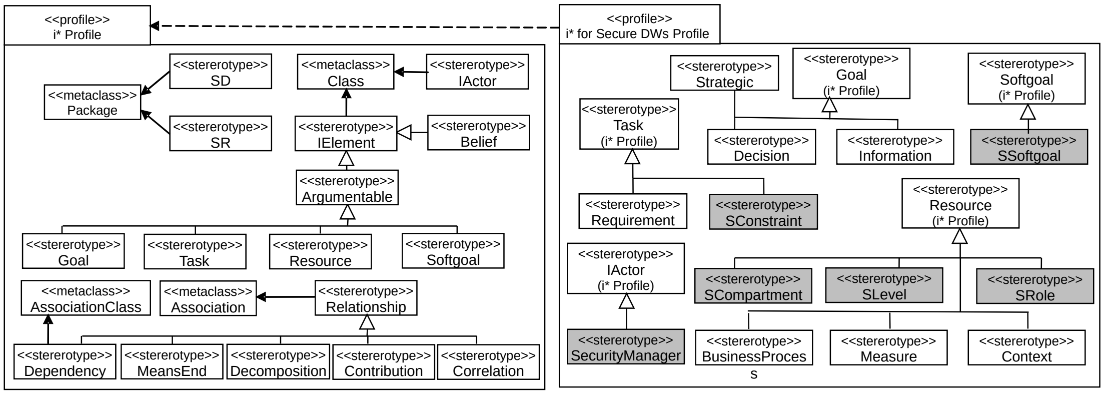

<<profile>>
i* Profile
<<profile>>
i* for Secure DWs Profile
<<stererotype>> SD
<<metaclass>> Package
<<stererotype>> SR
<<metaclass>> Class
<<stererotype>> IActor
<<stererotype>> IElement
<<stererotype>> Belief
<<stererotype>> Argumentable
<<stererotype>> Goal
<<stererotype>> Task
<<stererotype>> Resource
<<stererotype>> Softgoal
<<metaclass>> AssociationClass
<<metaclass>> Association
<<stererotype>> Relationship
<<stererotype>> Dependency
<<stererotype>> MeansEnd
<<stererotype>> Decomposition
<<stererotype>> Contribution
<<stererotype>> Correlation
<<stererotype>> Strategic
<<stererotype>> Goal (i* Profile)
<<stererotype>> Softgoal (i* Profile)
<<stererotype>> Task (i* Profile)
<<stererotype>> Decision
<<stererotype>> Information
<<stererotype>> SSoftgoal
<<stererotype>> Requirement
<<stererotype>> SConstraint
<<stererotype>> Resource (i* Profile)
<<stererotype>> IActor (i* Profile)
<<stererotype>> SCompartment
<<stererotype>> SLevel
<<stererotype>> SRole
<<stererotype>> SecurityManager
<<stererotype>> BusinessProces s
<<stererotype>> Measure
<<stererotype>> Context

Fig. 3. Overview of the profiles for i* modeling in the DW domain. The shaded elements are described in Sec. IV-B

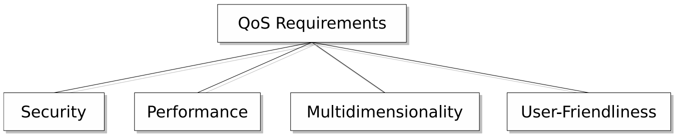


Fig. 4. Issues to be considered during data warehouse design

aspect, it is mandatory to use a framework of QoS requirements in DW. Figure 4 shows a framework for capturing the many different aspects that must be considered when designing a DW. The figure is based on the type catalogue for non-functional requirements for DW design introduced by [14]:

- **Security:** includes requirements related to the protection of valuable assets in the DW. Security requirements describe how the access is managed, what information can be accessed by whom, and under what condition that information can be accessed. We recall that, in this paper, security requirements are considered as those related to access control and audit issues.
- **Performance:** can be divided into performance regarding time (i.e. processing time or response time) and space (amount of memory used, main memory or secondary memory).
- **Multidimensionality:** covers all issues of access to multidimensional data, such as interpretability, integrability, timeliness, etc.
- **User-Friendliness:** finally requires flexibility, operability, and learnability.

We would like to point out that this is not a complete list of QoS requirements, but a representative one. The purpose of this is to attract attention to the need of modeling QoS requirements together with information requirements in an overall approach for DW development. Every concept in the framework presented here must be analyzed at the requirements level. New techniques have to be introduced for specifying such QoS requirements in the CIM together with the information requirements. In this paper we focus on one of the most important QoS requirements for DWs: *Security*.

IV. Security Requirements for Data Warehousing

Every kind of QoS requirement needs its own special kind of technique to be specified in a CIM. In this paper, we focus on security requirements.

Security requirements are QoS requirements associated with the protection of valuable assets in the system. These security requirements describe how access is managed, what information can be accessed by whom, and under what conditions information can be accessed, thus they are often called Access Control Policies (ACP).

An ACP approach for DWs is described in [4], [5], where the authors defined the Access Control and Audit (ACA) model in order to specify security issues for DWs. However, this approach is isolated from the DW requirement analysis stage and it may cause a misalignment between the security and privacy policies and the DW implementation. Many researchers have recognized the need to bridge the gap between requirements analysis and access control specification [1] by addressing security requirements in the development of software systems. Therefore, in following subsections, we focus on describing how to align the ACA model with QoS requirement analysis.

A. Access Control and Audit (ACA) model

The ACA model [4], [5] describes an access control mechanism, thus allowing us to represent confidentiality and audit measures of DWs by classifying subjects and objects in the system[3]. The classification uses access classes on the basis of three different but compatible ways of classifying users: by their *security level*, by the *role* and by the *compartments* they belong to. The access class is one element of a partially ordered set of classes, where an access class c1 dominates an access class c2 *if and only if* the security level of c1 is greater than or equal to that of c2, the compartments of c1 include those of c2, and at least one of the user roles of c1 (or one of its ancestors) is defined for c2. The following classes are described in order to be able to specify the ACA model:

- **Security user roles** are used by a company to organize users in a hierarchical role structure, according to the responsibilities of each type of work. Each user can play more than one role.
- **Security levels** indicate the clearance level of the user. Usually, an element of a hierarchically ordered set, such as Top Secret (TS), Secret (S), Confidential (C), and Unclassified (U), where $TS > S > C > U$.
- **Security user compartments** are also used by an organization to classify users into a set of horizontal compartments or groups, such as geographical location, area of work, etc. Each user can belong to one or more compartments.

B. Modeling security requirements

For specifying security requirements in a CIM, we need to extend the *i** framework for information requirements (Section III-A). Our new extension of *i** (see shaded elements in Figure 3) offers mechanisms to represent a special actor Security Manager (*SecurityManager*, ◯), who is the person in charge of the security in the organization. Security requirements are QoS requirements and they can be modeled by using i* softgoals (*SSoftgoal*, ☁). These softgoals represent and refine the security policy of the organization. The elements of the ACA model are considered as resources and labeled as `<<SCompartment>>`, `<<SLevel>>` and `<<SRole>>`. Moreover, in order to specify constraints for resources, we introduce a special task, labeled as `<<SConstraint>>`, which contributes to fulfil softgoals through the contribution link (*Contribution*, →—). We model the refinement process of softgoals by means of means-end links. Finally, each softgoal is related to *compartments*, *levels*, or *roles*) by means of decomposition links.

We propose the following two phases for establishing the ACA model from the security requirements, once we have the first *i** model with information requirements (see Section III-A):

- **Organization-based Security Analysis.** This phase consists on specifying a security requirement model and comprises three steps:
  1) Detect vulnerabilities and necessities for the system according to organization policies, laws, rules and regulations.
  2) Obtain the security requirements of the security manager by using well-known requirement elicitation mechanisms such as interviews. These requirements are modeled as softgoals and refined into lower-level softgoals. During the refinement process different responsibilities and tasks are discovered (i.e. roles and compartments) and the levels that will be used.
  3) Associate softgoals with the corresponding resources (i.e., *SCompartment*, *SRole* and *SLevel*).
- **Goal/Softgoal Analysis.** So far, we have obtained an information requirement model and a security requirement model. The next step is to relate both:
  1) Each refined softgoal is associated with the corresponding elements from the information requirement model (i.e. *Business Process*, *Measure* and *Context*).

[3] The ACA model also allows us to define Sensitive Information Assignment Rules (SIARs) in order to specify the security information of each element DW, rules for representing authorization rules (AURs), which work together with SIARs, and rules which allow us to specify audit requirements (ARs). However, this advance topic is out of the scope of this paper.

2) Consider other additional security issues for the modeled information requirements via the definition of *SConstraint* tasks. These tasks are associated with softgoals to indicate that contributes positively to their fulfillment.

C. Sample Application of our Approach

We provide a small example to illustrate the use of our approach. A pharmaceutical consortium manages several pharmacies. It wishes to analyze the sales of medicines by means of the medical prescriptions. Then, our focus is on the sales business process. Within the consortium there exist several groups: (i) a pharmacovigilance group that guards the proper use of certain medicines, (ii) a committee that cares for the health of the customers, and (iii) a commercial group devoted to dealing with medicines.

1) Information Requirements Analysis: This first phase is performed by using the approach described in Section III-A to model information requirements. The defined *i** model is shown in Figure 2. The business process *Sales_Prescription* is related to one main actor, the *marketing manager*, via the strategic goal *“increase prescription sales”*. From this strategic goal, two different decision goals are derived *“decrease prescription price”* and *“give incentive to pharmacist”*. From these decision goals, the following information goals have been obtained: *“analyze prescription price”* and *“analyze prescription sales”*. The derived information requirements are as follows (shown as tasks in Figure 2): *“analyze price by patient, prescription and pharmacy”*, and *“analyze sales by pharmacy, prescription and pharmacy_type”*. Furthermore, several resources are associated with the information requirements as measures and context of analysis. The measures are *sales* and *price*. The elements that represent the context of analysis are *patient*, *prescription*, and *pharmacy*. *Pharmacy_type* also belongs to the context of analysis and represents a way to aggregate the *pharmacy* data.

2) Organization-based Security Analysis: This phase is performed according to the proposal described in Section IV-B. The model is shown in Figure 5. We focus on the sales prescription process as security policy, which is performed by the security manager actor via the softgoal *“guarantee the security for the sales prescription process”*. By using a refinement process, three new softgoals *“guard the security of the use of certain medications and consumers’ rights”*, *“keep privacy for sales, price and patient’s data”*, and *“impose a clearance level to prescription process”* are obtained. During this process several responsibilities are discovered. Therefore, several security resources are discovered and associated with their corresponding softgoals (see Figure 5):

1) Hierarchical relations are obtained: *PharmacyEmployee*, which is then specialized into the *Pharmacist (Pharma)* and *Administrative (Admin)* roles.
2) Horizontal groups (compartments) are detected: *pharmacovigilanceCenter (pharmaC)* and *commercialManagerCenter*.
3) Restriction levels are established by means of *TopSecret* and *Secret*.

3) Goal/Softgoal Analysis: We need to associate resources obtained in information requirements analysis (i.e. *sales_prescription*, *sales*, *price*, *patient*, *prescription*, *pharmacy* and *pharmacy_type*) with the softgoals obtained from Security organizational-based analysis (e.g. *“guarantee the secure use of medication norms”* and *“impose maximum level of restriction to the sales prescription”*). The *security manager* depends on the *marketing manager* to achieve the mentioned softgoals (see Figure 6). *Sales_Prescription* is associated with the softgoal *“impose maximum level of restriction to the sales prescription”*, which have *TopSecret* as *SLevel*. Analogously, the context *prescription* is associated with the softgoal *“guarantee the secure use of medication norms”*, so it will have *PharmaC* as *SCompartment*. Due to the fact that *Sales_Prescription* and *Prescription* allow future refinements of the model, additional restrictions are needed. Figure 6 shows how the *SConstraint SRule* contributes to fulfil the three softgoals previously obtained, so it is associated with the business process *Sales_Prescription*. The same reasoning assures that the context *Prescription* will be related to a *SConstraint Audit*.

The benefit of applying our proposal is that the security levels, the security roles and the security compartments for every DW user are easily modeled in a CIM. Specifically, in our example we can conclude that, a user has access to *Sales_Prescription* if its access class dominates the access class of *Sales_Prescription*, i.e. its security level is *TopSecret*. This CIM can be used to derive a PIM [10] which reflects every security requirements, thus assuring that the implementation of the DW will satisfy users’ expectations.

V. Conclusion and Outlook

In this paper, we advocate the modeling of information and QoS requirements as an explicit stage in the development of a DW. Our point of view is that a DW that satisfies users’ expectations will be obtained if QoS requirements are modeled together with information requirements, from the early stages of the development onwards. Specifically, in this paper we have focused on security. Until now, we have proposed a general framework based on MDA [20], [21] in which we use our approaches for designing secure DWs at both conceptual [4], [5] and logical levels [19]. In this paper, we have focused on defining security requirements for DWs and the process for modeling security requirements, both introduced in Section IV.

As future work we will complete our approach for DW security requirements by defining new phases, such as a validation phase through the conceptual, logical and physical levels. It will comprise (i) the identification of malicious attempts and vulnerabilities, (ii) the refinement of the ACA model with new security rules, and (iii) an evaluation.

Furthermore, as security is only one aspect of QoS requirements for DWs, our future work includes to explore further aspects and how other QoS issues can be modeled during the

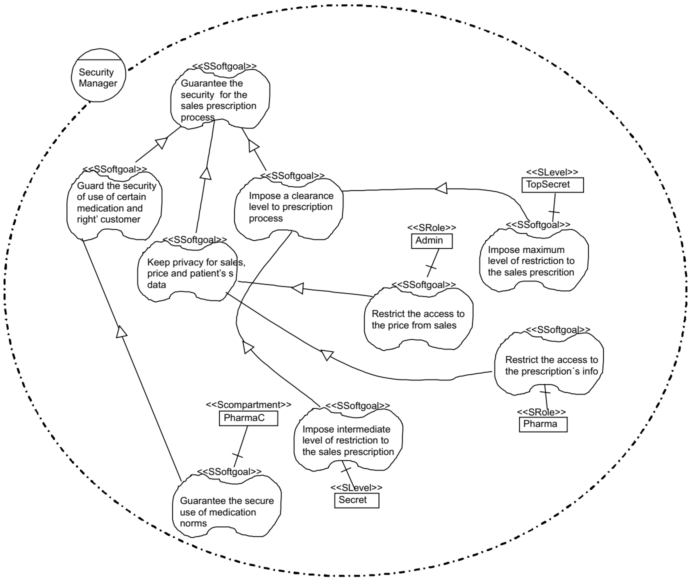

Security
Manager
<<SSoftgoal>>
Guarantee the security for the sales prescription process
<<SSoftgoal>>
Guard the security of use of certain medication and right' customer
<<SSoftgoal>>
Impose a clearance level to prescription process
<<SLevel>>
TopSecret
<<SSoftgoal>>
Impose maximum level of restriction to the sales prescrition
<<SRole>>
Admin
<<SSoftgoal>>
Keep privacy for sales, price and patient's s data
<<SSoftgoal>>
Restrict the access to the price from sales
<<SSoftgoal>>
Restrict the access to the prescription´s info
<<SRole>>
Pharma
<<Scompartment>>
PharmaC
<<SSoftgoal>>
Impose intermediate level of restriction to the sales prescription
<<SLevel>>
Secret
<<SSoftgoal>>
Guarantee the secure use of medication norms

Fig. 5. Model of security requirements (without information requirements)

requirements phase. Relationships and interdependencies between the different kinds of requirements will be investigated.

VI. Acknowledgements

This work has been supported by the METASIGN (TIN2004-00779) project from the Spanish Ministry of Science, and by the DADS (PBC-05-012-2) project from the Castilla-La Mancha Ministry of Science (Spain). Veronika Stefanov is funded by the Austrian Federal Ministry for Education, Science, and Culture, and the European Social Fund (ESF) under grant 31.963/46-VII/9/2002. Jose-Norberto Mazón is funded by the Spanish Ministry of Education and Science under a FPU grant (AP2005-1360).

References

[1] Antón, A.I., Earp, J.B., Carter, R.A.: Precluding incongruous behavior by aligning software requirements with security and privacy policies. Information and Software Technology **45**(14) 2003 967–977

[2] Chung L., Nixon B., Yu E. and Mylopoulos J.: Non-Functional Requirements in Software Engineering, Kluwer Academic Publishers, Boston/Dordrecht/London (2000).

[3] Devanbu, P., Stubblebine S.: Software engineering for security: a roadmap. In: A. Finkelstein, Editor, The Future of Software Engineering, ACM Press, New York (2000), pp. 227239.

[4] Fernández-Medina, E., Trujillo, J., Villarroel, R., Piattini, M.: Access control and audit model for the multidimensional modeling of data warehouses. Decision Support Systems **42**(3) 2006 1270–1289

[5] Fernández-Medina E., Trujillo J., Villarroel R., Piattini M.: Developing secure data warehouses with a UML extension. Inf. Syst. 32(6): 826-856 (2007)

[6] Ferrari, E., Thuraisingham B.: Secure database systems. In: M. Piattini and O. Daz, Editors, Advanced Databases: Technology Design, Artech House (2000).

[7] Giorgini, P., Rizzi, S., Garzetti, M.: Goal-oriented requirement analysis for data warehouse design. In: DOLAP 2005, 47–56

[8] Kimball, R., Ross, M.: The Data Warehouse Toolkit. Wiley & Sons (2002)

[9] Mazón, J.N., Trujillo, J., Serrano, M., Piattini, M.: Designing data warehouses: from business requirement analysis to multidimensional modeling. REBNITA 2005

[10] Mazón, J.N., Pardillo J., Trujillo, J.: A Model-Driven Goal-Oriented Engineering Approach for Data Warehouses. Workshop on Requirements, Intentions and Goals in Conceptual Modeling (RIGiM). ER Workshops 2007. Lecture Notes in Computer Science 4802, pp. 255-264.

[11] Mazón, J.N., Trujillo, J.: A Model Driven Modernization Approach for Automatically Deriving Multidimensional Models in Data Warehouses. 26th International Conference on Conceptual Modeling (ER 2007). Lecture Notes in Computer Science 4801, pp. 56-71

[12] Mazón, J.N., Trujillo, J.: An MDA approach for the development of data warehouses. Decision Support Systems. **doi:10.1016/j.dss.2006.12.003**

[13] Mazón, J.N., Trujillo, J., Lechtenbörger, J.: Reconciling requirement-driven data warehouses with data sources via multidimensional normal forms. Data & Knowledge Engineering. 63(3): 725-751 (2007)

[14] Paim, F.R.S., Castro, J.: Enhancing Data Warehouse Design with the NFR Framework. In WER 2002, 40–57

[15] Paim, F.R.S., Castro, J.: DWARF: An approach for requirements definition and management of data warehouse systems. In RE 2003, 75–84

[16] Prakash, N., Singh, Y., Gosain, A.: Informational scenarios for data warehouse requirements elicitation. ER 2004, Vol. 3288 of Lecture Notes in Computer Science, 205–216

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

[18] Sandhu, R. and Samarati P.: Authentication, access control, and intrusion detection. In: A. Tucker, Editor, CRC Handbook of Computer Science and Engineering, CRC Press Inc (1997).

[19] Soler E., Villarroel R., Trujillo J., Fernández-Medina E., Piattini M.: Representing Security and Audit Rules for DWs at the Logical Level by Using the Common Warehouse Metamodel. ARES 2006: 914-921

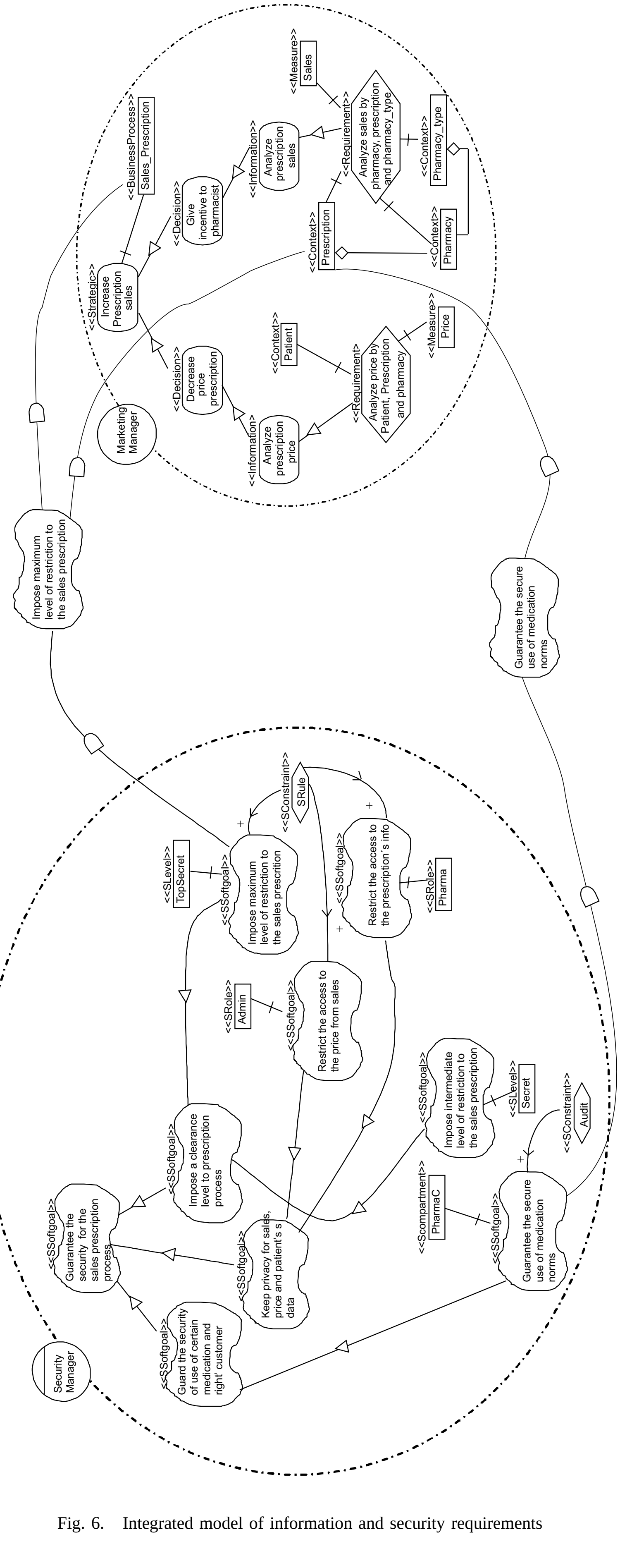
[20] Soler E., Trujillo J., Fernández-Medina E., Piattini M.: A Framework for the Development of Secure DWs based on MDA and QVT. ARES 2007, pp. 294-300

[21] Soler E., Trujillo J., Fernández-Medina E., Piattini M.: Aplicacin de QVT al Desarrollo de Almacenes de Datos Seguros: Un Caso de Estudio. IDEAS 2007. Isla Margarita (Venezuela).

[22] Stefanov, V, List, B.: A UML Profile for Modeling Data Warehouse Usage. In: 3rd International Workshop on Foundations and Practices of UML (FP-UML 2007). ER Workshops 2007. Lecture Notes in Computer Science 4802, pp. 137-147.

[23] Winter, R., Strauch, B.: A method for demand-driven information requirements analysis in data warehousing projects. HICSS 2003.

[24] Yu, E.: Towards modeling and reasoning support for early-phase requirements engineering. RE 1997, 226-235.



<<BusinessProcess>>
Sales_Prescription
<<Measure>>
Sales
<<Strategic>>
Increase Prescription sales
<<Decision>>
Give incentive to pharmacist
<<Information>>
Analyze prescription sales
<<Requirement>>
Analyze sales by pharmacy, prescription and pharmacy_type
<<Context>>
Pharmacy_type
<<Context>>
Prescription
<<Context>>
Pharmacy
<<Decision>>
Decrease price prescription
<<Context>>
Patient
<<Requirement>>
Analyze price by Patient, Prescription and pharmacy
<<Measure>>
Price
<<Information>>
Analyze prescription price
Marketing Manager
Impose maximum level of restriction to the sales prescription
Guarantee the secure use of medication norms
<<SConstraint>>
SRule
<<SLevel>>
TopSecret
<<SSoftgoal>>
Impose maximum level of restriction to the sales prescrition
<<SSoftgoal>>
Restrict the access to the prescription´s info
<<SRole>>
Pharma
<<SRole>>
Admin
<<SSoftgoal>>
Restrict the access to the price from sales
<<SSoftgoal>>
Impose intermediate level of restriction to the sales prescription
<<SLevel>>
Secret
<<SConstraint>>
Audit
<<SSoftgoal>>
Impose a clearance level to prescription process
<<SSoftgoal>>
Guarantee the security for the sales prescription process
<<SSoftgoal>>
Keep privacy for sales, price and patient's s data
<<Scompartment>>
PharmaC
<<SSoftgoal>>
Guarantee the secure use of medication norms
<<SSoftgoal>>
Guard the security of use of certain medication and right' customer
Security Manager
+
+
+
+

Fig. 6. Integrated model of information and security requirements