Un Profile de UML para Diseñar Almacenes de Datos Seguros

R. Villarroel, E. Fernández-Medina, J. Trujillo, M. Piattini

***Resumen*. Los Almacenes de Datos (*Data Warehouses*, DW's), Bases de Datos Multidimensionales y aplicaciones de Procesamiento Analítico En-Línea (*On-Line Analytical Processing*, OLAP) son usados como un mecanismo muy poderoso para descubrir información de negocio crucial en la toma de decisiones estratégicas de las empresas. Considerando de extrema importancia la información manejada por este tipo de aplicaciones, es esencial definir y hacer cumplir medidas de seguridad desde las etapas tempranas del diseño del DW. Además, la confidencialidad es un requisito especialmente importante para aplicaciones basadas en modelos multidimensionales (MD), ya que la información de negocio, que es muy sensible, puede ser descubierta ejecutando simples consultas. En los últimos años, se han propuesto una serie de aproximaciones para realizar el diseño conceptual de los DW's siguiendo el paradigma de modelado MD. Sin embargo, ninguna de estas propuestas considera la seguridad como un elemento importante en sus modelos, y por tanto, no permiten especificar restricciones de confidencialidad para ser cumplidas por las aplicaciones que usarán estos modelos MD. En este artículo, analizamos los problemas de confidencialidad de los DW's y presentamos un *profile* del Lenguaje de Modelado Unificado (UML) que nos permite especificar los principales aspectos de seguridad en el modelado conceptual MD, permitiendo diseñar DW´s seguros. Adicionalmente, mostramos los beneficios de nuestro *profile* aplicándolo a un ejemplo.**

***Palabras Clave*—Modelos de datos, seguridad, seguridad de datos, métodos orientados a objetos.**

I. Introducción

La seguridad de la información es un serio requisito que debe ser cuidadosamente considerado, no como un aspecto aislado, sino como un elemento que esté presente en todas las etapas del ciclo de vida del desarrollo, desde el análisis de requisitos hasta la implementación y mantenimiento [4], [6]. Se han propuesto diferentes ideas para la integración de la seguridad en el proceso de desarrollo de sistemas, pero sólo consideran la seguridad de la información desde un punto de vista criptográfico [9]. Chung et al. también enfatizan la integración de los requisitos de seguridad en el diseño, ofreciendo a los diseñadores modelos que especifican aspectos de seguridad, pero sin abordar temas específicos de bases de datos y DW´s [1]. MOMT [15] es una propuesta que trata de integrar la seguridad en el modelado conceptual, pero no cubre el proceso de desarrollo completo y no ha tenido mucho reconocimiento. Otra propuesta interesante es UMLsec [10], pero sólo trata con sistemas de información en general, mientras que el diseño conceptual de bases de datos y DW's no es considerado. Existe, también, una propuesta metodológica y un conjunto de modelos para diseñar bases de datos seguras [5] para ser implementadas con *Oracle9i Label Security* (OLS). Unida a la anterior metodología, la propuesta de un Lenguaje de Restricciones de Seguridad Orientado a Objetos (*Object Security Constraint Language*, OSCL) [16], permite especificar restricciones de seguridad en el proceso de diseño conceptual y lógico de bases de datos. Sin embargo, las propuestas anteriores no consideran el diseño de modelos MD seguros para DW`s.

En la literatura podemos encontrar diversas iniciativas para incluir seguridad en DW's [11], [12], [17], [18]. Muchas de ellas están enfocadas a aspectos específicos relacionados con el control de acceso, la seguridad multinivel, sus aplicaciones en bases de datos federadas, aplicaciones con herramientas comerciales, etc. Sin embargo, ninguna de ellas considera los aspectos de seguridad en todas las etapas del ciclo de desarrollo ni la introducción de la seguridad en el diseño conceptual MD. En cuanto al diseño de DW`s, veremos que varios enfoques se han propuesto para representar las principales propiedades MD a nivel conceptual [8], [19], [21]. Estas propuestas proporcionan sus propias notaciones gráficas no estándares, y ninguna de ellas ha sido ampliamente aceptada como un modelo conceptual estándar para el modelado MD. Recientemente otro enfoque [14], [20] ha sido propuesto para realizar el modelado conceptual MD orientado a objetos (OO). Esta propuesta es una extensión de UML (*profile*), que se define en base a los mecanismos de extensión estándar (estereotipos, valores etiquetados y restricciones) provistos por UML. Sin embargo, ninguno de estos enfoques de modelado MD considera la seguridad como un aspecto importante de sus modelos conceptuales, por lo que no resuelven el problema de la seguridad en estos tipos de sistemas.

La seguridad, y en concreto la confidencialidad, es un aspecto muy importante para los almacenes de datos, debido a que los constantes cambios en las peticiones de los usuarios y en las fuentes de datos obligan a una mayor flexibilidad, pero también a un mayor control en la confidencialidad de la información. Un aspecto importante a considerar en almacenes de datos, que lo diferencia de los sistemas operacionales, es que la información no se trata de forma estática, sino que cobra importancia la evolución de la misma a lo largo del tiempo, es decir, su historia, para lo cual deben establecerse

Esta investigación es parte de los proyectos CALIPO (TIC2003-07804-C05-C03) y RETISTIC (TIC2002-12487-E), soportados por la Dirección General de Investigación del Ministerio de Ciencia y Tecnología, y la red VII-J.RITOS2 financiada por CYTED.

los mecanismos que permitan la confidencialidad de tal cantidad de información.

En este artículo, presentamos un *profile* que nos permite representar la información de seguridad de los datos y restricciones de los DW's en el modelado MD a nivel conceptual. Esta propuesta se basa en el modelo de seguridad multinivel, considerando únicamente la operación de lectura (*read*) ya que ésta es la operación más común en aplicaciones de usuario final. Este modelo nos permite clasificar tanto la información como al usuario en clases de seguridad, y así hacer cumplir el control de acceso obligatorio. El uso de este enfoque, permite implementar los modelos MD seguros con cualquiera de los SGBD que son capaces de implementar bases de datos multinivel, tales como OLS [13] y DB2 Universal Database (UDB) [3].

El resto de este artículo se estructura así: En la sección II proponemos la nueva extensión de UML para el modelado MD seguro. La sección III ilustra un caso de estudio aplicando nuestra extensión de UML. Finalmente, en la sección IV presentamos las principales conclusiones e introducimos el trabajo futuro.

II. Extensión de UML para el Modelado Multidimensional Seguro

En este trabajo, nos basamos en un enfoque de modelado MD que utiliza UML para representar las propiedades estructurales de los modelos MD [14], [20]. El objetivo de nuestra extensión de UML es permitir que sea posible diseñar modelos conceptuales MD, pero clasificando la información para definir qué propiedades tiene que poseer el usuario para tener derecho a acceder a la información. Por tanto, consideramos tres etapas principales:

1) Definición precisa de la organización de usuarios que tendrá acceso al sistema MD. Podemos definir un nivel preciso de granularidad considerando tres formas de organización de usuarios: Niveles de seguridad (que indican el nivel de acreditación del usuario), Categorías de usuario (que indican una clasificación horizontal de usuarios atendiendo a ciertos criterios como de separación territorial, departamentos, etc.), y Roles de usuario (que indican una organización jerárquica de usuarios de acuerdo a sus roles o responsabilidades dentro de la organización).
2) Clasificación de la información del modelo MD. Podemos definir para cada elemento del modelo (clase de hecho, clase de dimensión, atributo de hecho, etc.) su información de seguridad, usando una tupla que esté compuesta de un intervalo de niveles de seguridad, un conjunto de categorías de usuario, y un conjunto de roles de usuario.
3) Cumplimiento del control de acceso obligatorio. Las operaciones típicas que los usuarios pueden ejecutar en este tipo de sistemas son operaciones de consulta. La regla de control de acceso para operaciones de lectura es la siguiente: Un usuario puede acceder a una información sólo si, a) el nivel de seguridad del usuario es mayor o igual que el nivel de seguridad de la información, b) todas las categorías de usuario que han sido definidas para la información están asignadas al usuario, y c) el usuario juega al menos uno de los roles que han sido definidos para la información.

Este artículo está enfocado en la segunda etapa, definiendo una extensión de UML que nos permite clasificar los elementos de seguridad en un modelo conceptual MD y especificar restricciones de seguridad. Debemos precisar también que la primera etapa se relaciona con aspectos de políticas de seguridad definidas en la organización por los administradores, lo que está fuera del alcance de este artículo.

De acuerdo a [2], una extensión de UML comienza con una breve descripción y a continuación se describen todos los estereotipos, valores etiquetados, y restricciones de la extensión. Además de estos elementos, una extensión contiene un conjunto de reglas bien formadas. Estas reglas ayudan a definir la consistencia semántica (desde un punto de vista estático) de la extensión. Por lo tanto, definimos nuestra extensión de UML siguiendo el esquema compuesto de los siguientes elementos: descripción, prerrequisitos de la extensión, nuevos tipos de datos, estereotipos / valores etiquetados, reglas bien formadas (definidas tanto en lenguaje natural como mediante un conjunto de invariantes definidas por medio de expresiones OCL), y comentarios. Para la definición de los estereotipos, seguimos la estructura que es sugerida en [7], la que está compuesta de un nombre, la metaclase base, la descripción, los valores etiquetados y una lista de restricciones definidas por medio de OCL. Para la definición de valores etiquetados, son definidos el tipo de valores etiquetados, la multiplicidad, la descripción, y el valor por defecto.

A. Descripción

Esta extensión de UML reutiliza un conjunto de estereotipos definidos previamente en [14], y define un conjunto de valores etiquetados, estereotipos y restricciones, que nos permiten crear modelos MD seguros. Los 20 valores etiquetados que hemos definido se aplican a ciertos componentes que son especialmente particulares del modelado MD (hechos, dimensiones, etc.), permitiéndonos representarlos en el modelo MD y en los mismos diagramas que describen el resto del sistema. Estos valores etiquetados representarán la información sensible (en base a los tipos de datos definidos) de los diferentes elementos del modelado MD, y nos permitirán especificar restricciones de seguridad dependiendo de la información de seguridad y del valor de los atributos de los elementos del modelo. El estereotipo *UserProfile* nos ayudará a identificar una clase especial que definirá el perfil de los usuarios del sistema. Un conjunto de reglas bien formadas definen la semántica del modelo. El uso correcto de nuestra extensión es asegurado por la definición de restricciones tanto en lenguaje natural como en OCL. De este modo, hemos definido 7 nuevos estereotipos: uno que especializa el elemento de modelo *Class*, dos que especializan el elemento de modelo *Primitive* y cuatro que especializan el elemento de modelo *Enumeration*.

En la Fig. 1 hemos representado porciones del metamodelo de UML para mostrar donde se ubican nuestros estereotipos. Sólo hemos representado las jerarquías de especialización,

debido a que el hecho más importante de un estereotipo es la clase base de la cual el estereotipo se especializa. En esta figura, los nuevos estereotipos se muestran en color gris oscuro, mientras que los estereotipos que reutilizamos a partir del perfil previo [14] están en un color gris claro y las clases propias de UML permanecen en blanco.

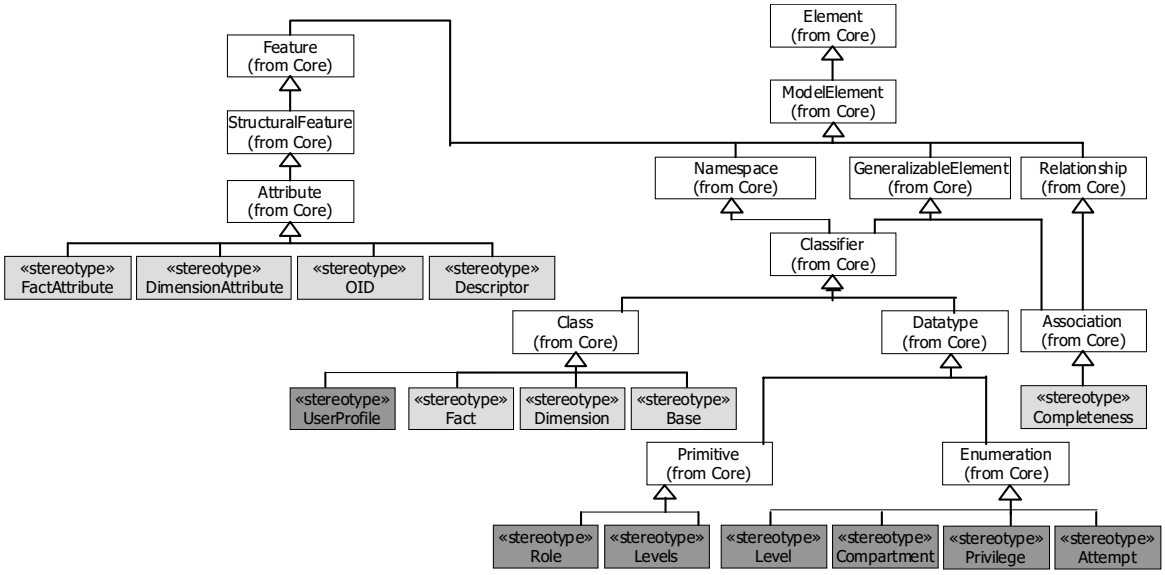


Fig. 1. Extensión de UML con estereotipos

B. Prerrequisitos de la Extensión

Este perfil de UML reutiliza estereotipos que fueron previamente definidos en otro *profile* de UML en [14]. Este perfil proporciona los estereotipos, valores etiquetados y restricciones que son necesarias para el cumplimiento de las propiedades del modelado MD conceptual. Para facilitar la comprensión del *profile* de UML que presentamos y usamos en este artículo, ofrecemos un resumen de la especificación de estos estereotipos en la Tabla I.

C. Tipos de Datos

Necesitamos la definición de algunos tipos de datos nuevos (ver Fig. 2) que serán usados en nuestras definiciones de valores etiquetados. En la Fig. 1 podemos ver las clases base de las cuales estos nuevos estereotipos se especializan.

TABLA I
STEREOTIPOS DEL PROFILE DE UML PARA EL MODELADO CONCEPTUAL MD

Nombre	Clase Base	Descripción
Fact	Class	Clases de este estereotipo representan hechos en un modelo MD
Dimension	Class	Clases de este estereotipo representan dimensiones en un modelo MD
Base	Class	Clases de este estereotipo representan niveles de jerarquía de dimensiones en un modelo MD
OID	Attribute	Atributos de este estereotipo representan atributos OID de clases Fact, Dimension o Base en un modelo MD
Fact-Attributes	Attribute	Atributos de este estereotipo representan atributos de clases Fact en un modelo MD
Descriptor	Attribute	Atributos de este estereotipo representan atributos descriptor de clases Dimension o Base en un modelo MD
Dimension-Attribute	Attribute	Atributos de este estereotipo representan atributos de clases Dimension o Base en un modelo MD
Completeness	Association	Asociaciones de este estereotipo representan la completitud de una asociación entre una clase Dimension y una clase Base o entre dos clases Base

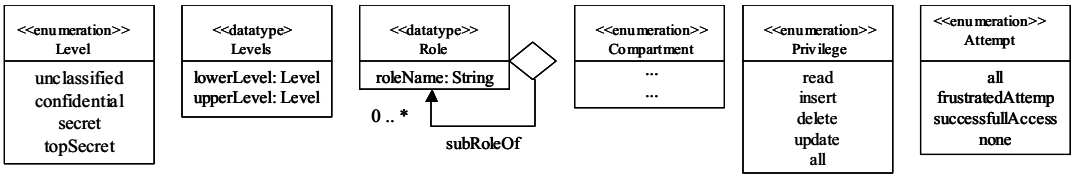


Fig. 2. Nuevos tipos de datos

El tipo Level será la enumeración ordenada compuesta por todos los niveles de seguridad que se han considerado (estos valores serán normalmente *unclassified*, *confidential*, *secret* y *top Secret*). El tipo *Levels* será un intervalo de niveles compuesto por un nivel mínimo y uno máximo. El tipo *Role* representará la jerarquía de los roles de usuario que se pueden definir para la organización (por simplicidad, no consideramos herencia múltiple). El tipo *Compartment* es la enumeración compuesta por todas las categorías de usuario que se han considerado en la organización. El tipo *Privilege* será una enumeración de todos los privilegios que han sido considerados (estos valores típicamente son *read*, *insert*, *delete*, *update*, *all*). El tipo *Attempt* será una enumeración de todos los tipos de acceso que han sido considerados (estos valores, son *all*, *frustratedAttempt*, *successfullAccess*, *none*).

D. Valores Etiquetados

En esta sección, mostramos la definición de diversos valores etiquetados de la extensión. La Tabla II muestra 14 de los 20 valores etiquetados que forman la extensión. Los 6 restantes son SecurityLevel, SecurityRoles y SecurityCompartments aplicados (con la misma semántica que a las clases) tanto a los atributos como a las instancias, y que por motivos de espacio no se han incluido en este artículo.

Todos los valores por defecto de valores etiquetados de seguridad del modelo son colecciones vacías. Por otro lado, el valor por defecto de valores etiquetados de seguridad para cada clase es la menos restrictiva (el menor nivel de seguridad, jerarquía de rol de seguridad que ha sido definida para el modelo y el conjunto vacío de categorías). El valor por defecto de los valores etiquetados de seguridad para los atributos es heredado de las clases a la cual pertenecen.

Si necesitamos especificar la situación en la que los accesos a la información de una clase tienen que ser registrados en un archivo log para una auditoría futura, deberemos usar los valores etiquetados *LogType* y *LogCond* en esa clase. Por defecto, el valor de *LogType* es *none*, de esta manera por defecto la auditoría no es necesaria. Por otro lado, si necesitamos especificar una restricción de seguridad, podemos usar OCL y el valor etiquetado *InvolvedClasses* para especificar en qué situación la restricción debe ser cumplida. Por defecto, el valor de este valor etiquetado es la clase con la cual la restricción está asociada. Finalmente, si necesitamos especificar una restricción de seguridad en la que un usuario o un conjunto de usuarios (dependiendo de una condición) puede o no acceder a la clase correspondiente, independientemente de la información de seguridad de esa clase, debemos usar excepciones unidas a los siguientes valores etiquetados: *InvolvedClasses*, *ExceptSign*, *ExceptPrivilege* y *ExceptCond*. El valor por defecto de *InvolvedClasses* es la propia clase. Para *ExceptSign* el valor por defecto es +, y para *ExceptPrivilege* es *Read*.

TABLA II VALORES ETIQUETADOS DE LA EXTENSIÓN[A]

Valores Etiquetados del Modelo			
Nombre	Tipo	M	Descripción
classes	Set(OclType)	1..*	Especifica todas las clases del modelo. Este nuevo valor etiquetado es útil para navegar a través de todas las clases del modelo.
securityLevels	Sequence (Levels)	1..*	Especifica todos los niveles de seguridad que pueden ser usados por los elementos del modelo (ordenados desde el menos al más restrictivo).
securityRoles	Role	0..*	Especifica la estructura de roles jerárquica que ha sido definida para la organización. Este tipo será administrado como un árbol.
security-Compartments	Set (Compartment)	0..*	Especifica el conjunto de categorías que han sido definidas para la organización.

[A] M se refiere a Multiplicidad

TABLA II VALORES ETIQUETADOS DE LA EXTENSIÓN (CONTINUACIÓN)

Valores Etiquetados de la Clase			
Nombre	Tipo	M	Descripción
SecurityLevels	Levels	1..*	Especifica el intervalo de posibles valores de niveles de seguridad que una instancia de esta clase puede recibir. Si el nivel superior e inferior son iguales, todas las instancias tendrán el mismo nivel de seguridad. En caso contrario, el nivel de seguridad de la instancia en concreto será definida de acuerdo a una restricción de seguridad.
SecurityRoles	Set(Role)	0..*	Especifica un conjunto de roles de usuario. Cada rol es la raíz de un subárbol de la jerarquía de roles de usuario general definida para la organización. Todas las instancias de esta clase pueden tener los mismos roles de usuario, o pueden ser subárboles de los roles que han sido definidos para la clase. Una restricción de seguridad puede decidir los roles de usuario para cada instancia de acuerdo al valor de algunos atributos de la instancia.
Security-Compartments	Set (Compartment)	0..*	Especifica un conjunto de categorías. Todas las instancias de esta clase pueden tener las mismas categorías de usuario, o un subconjunto de ellas. Una restricción de seguridad puede decidir las categorías de usuario para cada instancia de acuerdo al valor de algunos atributos de la instancia.
LogType	Attempt	0..1	Especifica si el acceso debe ser registrado: ninguno, todos los accesos, sólo accesos frustrados, o sólo accesos satisfactorios.
LogCond	OCLExpression	0..1	Especifica la condición para que el acceso sea registrado.
Involved-Classes	Set(OclType)	0..*	Especifica las clases que deben estar involucradas en una consulta para hacer cumplir una excepción.
ExceptSign	{+,-}	0..1	Especifica si una excepción permite (+) o rechaza (-) el acceso a las instancias de esta clase a un usuario o a un grupo de usuarios.
Except-Privilege	Set(Privilege)	0..*	Especifica los privilegios que el usuario puede recibir o perder.
ExceptCond	OCLExpression	0..*	Especifica la condición que los usuarios deben cumplir para ser afectados por esta excepción.
Valores Etiquetados de la Restricción			
Nombre	Tipo	M	Descripción
Involved-Classes	Set(OCLType)	0..*	Especifica las clases que están involucradas en una consulta, las que deben ser cumplidas en la restricción.

E. Estereotipos

Necesitamos definir un estereotipo para especificar otros tipos de restricciones de seguridad (ver Tabla III). El estereotipo *UserProfile* puede ser necesario para especificar restricciones dependiendo de una información particular de un usuario o un grupo de usuarios, por ejemplo, dependiendo de la nacionalidad del usuario, edad, etc. Así, los tipos de datos y valores etiquetados definidos previamente, se aplicarán a los estereotipos F*act*, *Dimension* y *Base* para considerar otros aspectos de seguridad.

TABLA III
ESTEREOTIPO USER PROFILE DE NUESTRA EXTENSIÓN

Nombre	**UserProfile**
Clase base	Class
Descripción	Clases de este estereotipo contienen todas las propiedades que los sistemas administran de los usuarios.
Restricciones	- Esta clase no está asociada con otras clases Self.AssociationsEnd.size()=0 - No hay más de una clase de este tipo **Context** Model **Inv** self.classes->forAll(oclisTypeOf(UserProfile))->size()<=1 - El nombre de la clase de este estereotipo será *PerfilUsuario* self.className=*PerfilUsuario*
Valores Etiquetados	Ninguno
Icono	

F. Reglas bien Formadas

Hemos identificado y especificado tanto en lenguaje natural como en OCL un conjunto de reglas bien formadas que describen la semántica estática del modelo. En este artículo, por restricciones de espacio no se incluye un detalle de cada regla. Estas reglas están agrupadas básicamente de la siguiente forma:

- Valor correcto de los valores etiquetados.
- La información de seguridad de las instancias.
- Relaciones entre la información de seguridad de las clases y sus atributos.
- Categorización de las dimensiones.
- Jerarquías de clasificación.
- Atributos derivados.
- Combinación de dimensiones.

G. Comentarios

Además de las reglas bien formadas (que en realidad son restricciones inherentes al modelo) identificadas, el diseñador puede especificar restricciones de seguridad con OCL. Si la información de seguridad de una clase o de un atributo depende del valor de un atributo de una instancia, éste puede ser expresado como una expresión OCL (ver Figura 4). Normalmente, las restricciones de seguridad definidas para estereotipos de clases (hecho, dimensión y base) serán definidas usando una nota de UML asociada a la clase correspondiente. No imponemos más restricciones al contenido de estas notas que sólo aquéllas impuestas por las definiciones de los valores etiquetados, de manera que permitan al diseñador una mayor flexibilidad.

III. CASO DE ESTUDIO

En esta sección, aplicamos nuestra extensión para el diseño conceptual de un modelo MD seguro en el contexto de un sistema de salud típico. Hemos considerado un ejemplo reducido para poder enfocar nuestra atención en las especificaciones de seguridad. La Fig. 3 (a) muestra la jerarquía simplificada de roles de usuario del sistema, y la Fig. 3 (b) muestra los niveles de seguridad que han sido definidos. En este ejemplo no hemos considerado categorías de usuario.

La Figura 4 muestra un modelo MD que incluye una clase de hecho (Admisión), dos dimensiones (Diagnóstico y Paciente), dos clases base (Grupo_Diagnos y Ciudad), y una clase (PerfilUsuario).

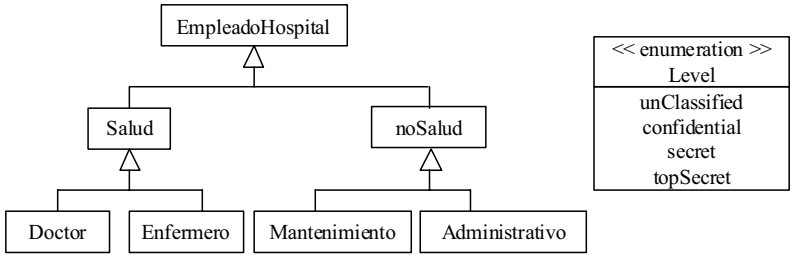


Fig. 3. (a) Jerarquía de roles de usuario (b) Niveles de seguridad

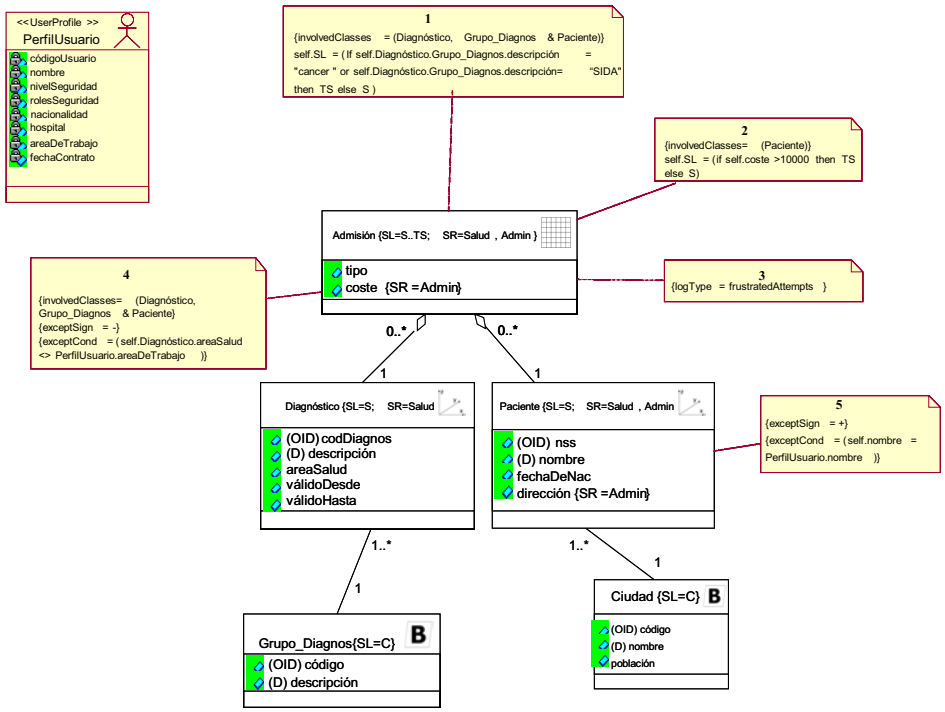


Fig. 4.Ejemplo de modelo multidimensional con información y restricciones de seguridad

La clase PerfilUsuario (estereotipo UserProfile) contiene la información de todos los usuarios que tendrán acceso a este modelo multidimensional. La clase de hecho Admisión –estereotipo *Fact*- contiene todas las admisiones individuales de pacientes en uno o más hospitales, y puede ser accedido por todos los usuarios que tienen niveles de seguridad *secret* o *topSecret* -valor etiquetado *SecurityLevels* (SL) de las clases-, y juegan roles de salud o administrativo -valor etiquetado *SecurityRoles* (SR) de las clases-. Note que el atributo *coste* puede ser sólo accedido por usuarios que juegan rol de *administrativo* –valor etiquetado SR de los atributos- La dimensión Paciente contiene la información de los pacientes del hospital y puede ser accedido por todos los usuarios que tienen nivel de seguridad secreto –valor etiquetado SL-, y juegan roles de salud o administrativo –valor etiquetado SR-.

El atributo Dirección puede ser accedido sólo por usuarios que juegan el rol de administrativo –valor etiquetado SR de los atributos-. La clase base Ciudad contiene la información de las ciudades, y nos permite agrupar a grupos de pacientes por ciudades. Las ciudades pueden ser accedidas por todos los usuarios que tienen nivel de seguridad *confidential* –valor etiquetado SL-. La dimensión Diagnóstico contiene la información de cada diagnóstico, y puede ser accedida por los usuarios que juegan un rol de salud –valor etiquetado SR-, y tienen nivel de seguridad secreto –valor etiquetado SL-. Finalmente, Grupo_Diagnos contiene un conjunto de grupos generales de diagnóstico. Cada grupo puede estar relacionado con varios diagnósticos, pero un diagnóstico siempre estará relacionado a un grupo. Los grupos de diagnóstico pueden ser accedidos por todos los usuarios que tienen nivel de seguridad *confidential* –valor etiquetado SL-.

Se han especificado varias restricciones de seguridad utilizando las restricciones, estereotipos y valores etiquetados definidos previamente:

1) El nivel de seguridad de cada instancia de Admisión es definido por una restricción de seguridad especificada en el modelo. Si el valor del atributo descripción de Grupo_Diagnos a la cual pertenece el diagnóstico que está relacionado a la Admisión es cáncer o SIDA, el nivel de seguridad –valor etiquetado SL- de esta admisión será *topSecret*, en caso contrario será *secret*. Esta restricción es sólo aplicada si el usuario hace una consulta cuya información viene de la dimensión Diagnóstico o de la clase base Grupo_Diagnos, unida con la dimensión Paciente –valor etiquetado involvedClasses-. De esta manera, un usuario que tiene un nivel de seguridad secreto podría obtener el número de pacientes con cáncer por cada ciudad, pero nunca si la información de la dimensión Paciente aparece en la consulta.
2) El nivel de seguridad –valor etiquetado SL- de cada instancia de Admisión puede también depender del valor del atributo *coste*, que indica el precio del servicio de admisión. En este caso, la restricción es sólo aplicable para consultas que contienen información de la dimensión Paciente –valor etiquetado *involvedClasses*-.
3) El valor etiquetado *logType* ha sido definido para la clase Admisión, especificando el valor *frustratedAttempts*. Este valor etiquetado especifica que el sistema tiene que registrar, para una auditoría futura, la situación en la cual

un usuario trata de acceder a información de esta clase de hecho, y el sistema lo rechaza debido a la carencia de los permisos necesarios.

4) Por razones de confidencialidad, podemos denegar el acceso a información de admisión a usuarios cuya área de trabajo es diferente del área de una instancia de admisión particular. Esto se especifica con una excepción en la clase de hecho Admisión, y con los valores etiquetados *involvedClasses*, *exceptSign* y *exceptCond*.
5) Los pacientes podrían ser usuarios especiales del sistema. En este caso, debería ser posible que los pacientes accedan a su propia información como pacientes (por ejemplo, consultando sus datos personales). Esta restricción es especificada usando los valores etiquetados *exceptSign* y *exceptCond* en la clase Paciente.

El privilegio considerado en estas excepciones es *read*, pero no la hemos especificado en el modelo ya que es el valor por defecto del valor etiquetado *exceptPrivilege*.

Note que, usando esta extensión, es posible especificar un amplio rango de restricciones de confidencialidad en el modelado conceptual MD.

IV. Conclusiones y Trabajo Futuro

En este artículo hemos presentado una extensión de UML que nos permite representar los principales aspectos de seguridad en el modelado conceptual de almacenes de datos. Esta extensión contiene los estereotipos, valores etiquetados y restricciones necesarios para un modelado MD completo y potente. Estos nuevos elementos nos permiten especificar aspectos de seguridad tales como niveles de seguridad en los datos, categorías y roles de usuario sobre los principales elementos de un modelado multidimensional tales como hechos, dimensiones y jerarquías de clasificación. Hemos usado OCL para especificar las restricciones asociadas a estos nuevos elementos definidos, evitando así un uso arbitrario. La principal ventaja de este enfoque es que utilizamos UML, un lenguaje de modelado ampliamente aceptado, que ahorra a los diseñadores el esfuerzo de aprendizaje de un nuevo modelo y sus notaciones correspondientes para un modelado MD específico. Además, UML nos permite representar algunas propiedades MD que son difícilmente representadas en otras propuestas de modelado conceptual MD.

Nuestra aportación al área de modelado de la seguridad en sistemas de información y bases de datos, radica principalmente en una solución basada en un *profile*. Además, el uso de esta extensión facilitará la implementación en algunos de los SGBD que tienen la capacidad para implementar bases de datos multinivel, tales como Oracle Label Security y DB2 Universal Database. Considerando que los almacenes de datos, bases de datos multidimensionales y aplicaciones OLAP son usadas como mecanismos muy poderosos para el descubrimiento de información de negocio crucial en los procesos de toma de decisiones estratégicas, esta propuesta provee avances interesantes en la mejora de la seguridad de los sistemas de soporte a las decisiones y a la protección de información sensible que generalmente gestionan estos sistemas.

Nuestro trabajo futuro inmediato es generar código que nos permita definir las estructuras que albergarán los datos del almacén en una plataforma destino como por ejemplo Oracle, incluyendo los aspectos de seguridad definidos en este artículo. Ello nos permitirá obligar a que las reglas definidas a nivel conceptual se cumplan para todos los usuarios que accedan a los datos del almacén. Un trabajo futuro más lejano es extender esta propuesta para poder considerar los procesos ETL (*Extraction-Transformation-Loading*) tan cruciales en el campo de los almacenes de datos.

V. Agradecimientos

Agradecemos a Sergio Luján-Mora por su participación en la especificación del *profile* de UML requerido para los prerrequisitos necesitados en este *profil*e.

VI. Referencias

[1] L. Chung, B. Nixon, E. Yu, y J. Mylopoulos, *Non-functional requirements in software engineering*, Boston/Dordrecht/London: Kluwer Academic Publishers, 2000.

[2] J. Conallen, *Building Web Applications with UML.* Object Technology Series. Addison-Wesley, 2000.

[3] S. Cota, *For Certain Eyes Only.* DB2 Magazine, 2004. 9(1): pp. 40-45.

[4] P. Devanbu yS. Stubblebine, *Software engineering for security: a roadmap*, en *The Future of Software Engineering*, A. Finkelstein, Editor, ACM Press, 2000, pp. 227-239.

[5] E. Fernández-Medina y M. Piattini. "*Designing Secure Database for OLS"*, en Actas 2003 *Database and Expert Systems Applications: 14th International Conference (DEXA 2003)*. Prague, Czech Republic: Springer.

[6] E. Ferrari y B. Thuraisingham, *Secure Database Systems*, en *Advanced Databases: Technology Design*, M. Piattini y O. Díaz, Editores, Artech House: London, 2000.

[7] M. Gogolla y B. Henderson-Sellers. "*Analysis of UML Stereotypes within the UML Metamodel"*, en Actas 2002 *5th International Conference on the Unified Modeling Language - The Language and its Applications.* Dresden, Germany: Springer, LNCS.

[8] M. Golfarelli y S. Rizzi. "*A Methodological Framework for Data Warehouse Design"*, en Actas 1998 *1st International Workshop on Data Warehousing and OLAP (DOLAP'98)*. Maryland, USA.

[9] A. Hall y R. Chapman, *Correctness by Construction: Developing a Commercial Secure System.* IEEE Software 19(1): pp. 18-25. Ene-Feb 2002.

[10] J. Jürjens. "UMLsec: Extending UML for secure systems development", en Actas 2002 - The Unified Modeling Language, Model Engineering, concepts and tools (UML 2002)-. Dresden, Germani: Springer-Verlag.

[11] N. Katic, G. Quirchmayr, J. Schiefer, M. Stolba, y A. Min Tjoa. "*A Prototype Model for Data Warehouse Security Based on Metadata"*, en Actas 1998 *9th International Workshop on Database and Expert Systems Applications (DEXA'98).* Vienna, Austria.: IEEE Computer Society.

[12] R. Kirkgöze, N. Katic, M. Stolda, y A. Min Tjoa. "*A Security Concept for OLAP"*, en Actas 1997 *8th International Workshop on Database and Expert System Applications (DEXA'97)*. Toulouse, France: IEEE Computer Society.

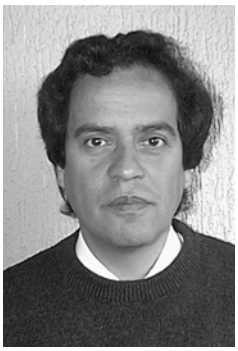
[13] J. Levinger, *Oracle label security. Administrator's guide. Release 2 (9.2)*. 2002. [OnLine] Disponible: http://www.csis.gvsu.edu/GeneralInfo/Oracle/network.920/a96578.pdf.

[14] S. Luján-Mora, J. Trujillo, y I.Y. Song. "*Extending the UML for Multidimensional Modeling"*, en Actas 2002 *5th International Conference on the Unified Modeling Language (UML 2002)*. Dresden, Germani: Springer-Verlag.

[15] D. Marks, P. Sell, y B. Thuraisingham, *MOMT: A multi-level object modeling technique for designing secure database applications.* Journal of Object-Oriented Programming. 9(4): pp. 22-29. Mar-Abr. 1996.

[16] M. Piattini y E. Fernández-Medina. "*Specification of security constraints in UML*", en Actas 2001 *35th Annual 2001 IEEE International Carnahan Conference on Security Technology*. London, United Kingdom.
[17] T. Priebe y G. Pernul. "*Towards OLAP Security Design - Survey and Research Issues.",* en Actas 2000 *3rd ACM International Workshop on Data Warehousing and OLAP (DOLAP'00)*. Washington DC, USA.
[18] A. Rosenthal y E. Sciore. "*View Security as the Basic for Data Warehouse Security.",* en Actas 2000 *2nd International Workshop on Design and Management of Data Warehouse (DMDW'00)*. Sweden.
[19] C. Sapia, M. Blaschka, G. Höfling, y B. Dinter. "*Extending the E/R Model for the Multidimensional Paradigm"*, en Actas 1998 *1st International Workshop on Data Warehouse and Data Mining (DWDM'98)*. Singapore: Springer-Verlag.
[20] J. Trujillo, M. Palomar, J. Gómez, y I.Y. Song, *Designing Data Warehouses with OO Conceptual Models.* IEEE Computer, special issue on Data Warehouses, 2001(34): pp. 66-75.
[21] N. Tryfona, F. Busborg, y J. Christiansen. "*starER: A Conceptual Model for Data Warehouse Design"*, en Actas 1999 *ACM 2nd International Workshop on Data Warehousing and OLAP (DOLAP'99)*. Missouri, USA: ACM.

VII. BIOGRAFÍAS



Rodolfo Villarroel es Magíster en Ingeniería Informática de la Universidad Técnica Federico Santa María (Chile) y estudiante de doctorado en la Escuela Superior de Informática de la Universidad de Castilla-La Mancha, en Ciudad Real (España). Es profesor adjunto del Departamento de Computación e Informática de la Universidad Católica del Maule (Chile). Sus actividades de investigación son seguridad en almacenes de datos y sistemas de información, y mejoramiento de procesos de software. Autor de varios artículos de seguridad en almacenes de datos y mejoramiento del proceso de gestión de configuración de software. Pertenece a la Sociedad Chilena de Ciencias de la Computación (SCCC) y a la Red de Mejoramiento de Procesos de Software (SPIN-Chile). Su correo es rvillarr@spock.ucm.cl

Juan Trujillo es profesor en la Escuela de Informática de la Universidad de Alicante, España. Trujillo obtuvo su Doctorado en Informática en la Universidad de Alicante (España) el año 2001. Sus intereses de investigación incluyen modelado de bases de datos, diseño conceptual de almacenes de datos, bases de datos multidimensionales, OLAP, y análisis y diseño orientado a objetos con UML. Ha publicado artículos en conferencias internacionales y revistas tales como ER, UML, ADBIS, CaiSE, WAIM, Journal de Gestión de Bases de Datos (JDM) e IEEE Computer. Participa como miembro de Comité de Programa de varios talleres y conferencias tales como ER, DOLAP, DSS, y SCI. También ha participado como revisor de varias revistas tales como JDM, KAIS, ISOFT y JODS. Su correo de contacto es jtrujillo@dlsi.ua.es.

Eduardo Fernández-Medina es Doctor y Master en Informática. Es profesor asistente en la Escuela Superior de Informática de la Universidad de Castilla-La Mancha en Ciudad Real. Su actividad de investigación es seguridad en bases de datos, almacenes de datos, servicios web y sistemas de información. Y también en métricas de seguridad. Es coeditor de varios libros y capítulos de libros en estos temas, y tiene varias docenas de artículos en conferencias nacionales e internacionales. Participa en el grupo de investigación ALARCOS del Departamento de Informática en la Universidad de Castilla-La Mancha en Ciudad Real, España. Pertenece a varias asociaciones de investigación y profesionales (ATI, AEC, AENOR, IFIP WG11.3 etc.). Su correo es eduardo.fdezmedina@uclm.es.

Mario Piattini es Master y Doctor en Informática por la Universidad Politécnica de Madrid. Auditor de Sistemas de Información Certificado por la ISACA (Information System Audit and Control Association). Actualmente es Catedrático de Universidad en la Escuela Superior de Informática de la Universidad de Castilla-La Mancha en Ciudad Real. Autor de varios libros y artículos sobre bases de datos, ingeniería de software y sistemas de información. Pertenece al grupo de investigación ALARCOS del Departamento de Informática en la Universidad de Castilla-La Mancha, en Ciudad Real, España. Sus intereses de investigación son: diseño de bases de datos avanzadas, calidad de bases de datos, métricas de software, métricas orientadas a objeto, mantenimiento de software. Su correo es Mario.Piattini@uclm.es