Информационные технологии

УДК 004.65, 004.056

Механизм управления доступом к данным в условиях виртуальной внешней модели

В. А. Петров, О. Д. Долина, И. Л. Толмачев

Кафедра информационных технологий
Российский Университет Дружбы Народов
ул. Миклухо-Маклая, д. 6, Москва, Россия, 117198

В статье рассматривается проблема организации разграничения доступа к данным в информационных системах, построенных на основе реляционных баз данных, предназначенных для автоматизации управления предприятием. В данной статье вводятся необходимые определения и понятия для построения модели разграничения доступа к данным на уровне реляционной модели через формирование виртуальных внешних моделей базы данных.

Ключевые слова: управление доступом к данным, разграничение прав доступа в информационных системах, права доступа в реляционных базах данных, виртуальная внешняя модель.

1. Введение

Разграничение прав доступа в информационных системах, построенных на основе реляционных баз данных, является актуальной проблемой, с которой ежедневно сталкиваются разработчики и администраторы информационных систем. Для различных классов приложений используются либо базовые модели разграничения доступа [1–3], либо предлагаются новые решения и усовершенствования основных моделей [1, 4, 5].

Актуальность проблемы усиливается под воздействием следующих факторов:

- сложная структура схемы базы данных (например, системы для административного управления предприятиями);
- большое число пользователей информационной системы;
- широкий набор ограничений прав доступа к данным системы.

В данной работе предлагается подход к управлению доступом к данным, нацеленный на обеспечение:

- достоверности данных в информационной системе в условиях сложной структуры иерархии управления (много подразделений, взаимодействующих друг с другом);
- вариативности при реализации одинаковых по смыслу иерархий.

2. О реализации разграничения доступа

При проектировании системы в целом и реляционной модели данных планируется, к какой информации должны иметь доступ пользователи. Описание прав доступа выносится за пределы реляционной модели и реализуется либо средствами управления правами доступа СУБД, либо на уровне приложения, или комбинированием этих способов. Стандартными средствами управления правами доступа СУБД нельзя разграничить доступ к подмножествам записей отношений (по горизонтали), доступ определяется только для полей (по вертикали) [6–8]. На уровне приложения в зависимости от прав пользователя приложение предоставляет возможности для осуществления тех или иных действий. Реализацию прав доступа к БД также иногда частично или целиком выносят на уровень приложения.

Статья поступила в редакцию 3 апреля 2011 г.

В системах с широким набором ограничений прав доступа к данным, для детального описания этих прав, в реляционной модели БД создают дополнительные отношения, описывающие эти права и обеспечивающие возможность участия пользователей в работе с информацией. Таким образом, описание представления пользователя становится частью предметной области. В условиях отсутствия необходимых механизмов на уровне СУБД реализация управления правами доступа осуществляется на уровне приложения.

Распределением прав доступа, как правило, занимаются администраторы системы. При этом не всегда учитывается служебная иерархия и распределение обязанностей в отделах. В отделах может происходить перепоручение заданий или каких-то обязанностей другим служащим (от начальника подчинённому). Но в большинстве систем отсутствует или слабо развит механизм делегирования полномочий [3]. Для обеспечения этой возможности приходится задействовать администраторов системы (или разработчиков) в процессе эксплуатации, т.е. администратор системы становится участником формирования и принятия решения, выполняя только техническую функцию осуществления делегирования полномочий. Результатом этого являются возможные ошибки и задержки в принятии решений, а также затраты на использование дополнительного человеческого ресурса.

В данной работе рассматриваются средства, позволяющие вынести механизм разграничения доступа к данным на уровень схемы реляционной модели, сделать его независимым от структуры конкретной БД. Информация о правах доступа к данным, представляющая смысловое значение для рассматриваемой предметной области, сохраняется в реляционной БД через использование надстройки над схемой БД. При этом пользователь, входя в систему, получает доступ только к подмножеству данных, соответствующих его полномочиям в конкретный момент времени.

Для рассматриваемого класса задач предлагается разработка модели разграничения доступа, которая будет соответствовать предъявляемым к ней требованиям функциональности:

- доступ только к данным соответствующим функциям сотрудника;
- возможность описания полномочий непосредственных подчинённых самими пользователями;
- назначение полномочий в процессе функционирования без привлечения администраторов системы.

3. Понятие «Функциональная обязанность»

Анализ различных организационно-управленческих и организационно-технологических схем [1, 2, 4] показывает, что в реальной жизни сотрудники организаций выполняют определённые функции не от своего личного имени, а в рамках некоторой должности. Должность представляет некоторую обобщённую сущность, обладающую определённой функциональностью и определяющую место работника в организационной структуре (подчинённость, права и полномочия). Таким образом, в большинстве организационно-технологических схем права и полномочия предоставляются не конкретному сотруднику, а через назначение его на определённую должность, вместе с которой он и получает некоторый типовой набор прав и полномочий. Однако конкретизация этих полномочий зависит от подразделения организации, в котором данный сотрудник занимает должность.

В данной работе для описания прав доступа введём несколько понятий.

Под **функциональной обязанностью** (ФО) будем понимать набор полномочий, которыми может обладать персона, выполняющая набор логически связанных действий в рамках конкретного (постоянного или временного) подразделения организации. Одна персона может обладать множеством функциональных обязанностей, но производить какие-либо действия над данными (выполнять функции) в конкретный момент времени персона может, используя полномочия только одной функциональной обязанности.

Функциональная обязанность является описанием, по которому определяются конкретные объекты управления (подмножество данных), на которые распространяется влияние персоны в процессе работы.

Абстрагируя понятие ФО по определённым параметрам, которые будем называть **характеристическими атрибутами**, мы приходим к понятию **типа функциональной обязанности**.

Тип функциональной обязанности (ТФО) — это такое обобщение ФО, которое позволяет описать выполняемые функции абстрактным образом на этапе проектирования системы. В процессе эксплуатации происходит конкретизация функций, отвечающих правам и полномочиям конкретного исполнителя.

В структуре организаций имеются подразделения, которые в процессе управления обладают некоторым одинаковым набором функций, но объекты управления, к которым применяются эти функции, распределяются по-разному между сотрудниками подразделений. Для обобщения этих функций вне привязки к исполнителям мы и вводим понятие ТФО. С его помощью можно описывать выполняемые функции без уточнения кто именно должен их выполнять. Таким образом, ТФО должен нам позволить описать функции, а ФО конкретизирует выполнение этих функций по различным объектам управления.

4. Формальные определения из реляционной модели

Для удобства дальнейшего изложения напомним несколько базовых формальных определений из реляционной модели [9, 10].

Отношение R определяется именем, схемой (структурой) и телом (значением отношения).

Схема отношения $Sch\,[R]$ задаётся набором пар атрибут–домен:

$$Sch\,[R] = R(A_1 : D_1; ...A_n : D_n),$$

где A_i — атрибут; D_i — домен атрибута A_i; $i \in \overline{1,n}$.

Тело отношения — множество n-арных кортежей (записей).

Кортеж — множество пар атрибут-значение:

$$t = \langle A_1 : d_1; ...A_n : d_n \rangle,$$

где $d_i \in D_i$ — значение атрибута A_i; $i \in \overline{1,n}$.

В каждый момент времени тело отношения является подмножеством декартового произведения доменов его атрибутов:

$$Body\,[R] \subset A_1 : D_1 \times ... \times A_n : D_n;$$

где D_i — домен атрибута A_i; $i \in \overline{1,n}$.

Множество всех атрибутов всех отношений:

$$\mathrm{A} := \{A_j\}.$$

Связи — пары первичных и внешних ключей отношений:

$$L_{ij_k} = (PK_i; FK_{j_k}),$$

где $PK_i \in Sch\,[R_i]$ — первичный ключ отношения R_i, $FK_{j_k} \in Sch\,[R_j]$ — внешний ключ отношения R_j, k — показывает, что внешних ключей в отношении может быть несколько.

5. Модель разграничения доступа

Введём определения и рассмотрим несколько утверждений, на основе которых будет строиться модель разграничения доступа в системе.

Утверждение 1. Существует преобразование, позволяющее построить отображение данных, соответствующее полномочиям конкретного служащего в конкретный момент времени.

Тип функциональной обязанности задаёт множество функциональных обязанностей, характеризующихся одинаковыми функциями для различных объектов управления. Типы функциональных обязанностей определяются набором атрибутов, которые будем называть **характеристическими атрибутами**, выступающими параметрами при построении отображений (подмножеств) данных, соответствующих полномочиям конкретных должностей.

Под **характеристическими атрибутами** (ХА) будем понимать некоторые атрибуты модели, по которым осуществляется описание ТФО и конкретизации ФО. Набор характеристических атрибутов выделяется при проектировании схемы базы данных, в соответствии с назначением системы, и может изменяться и расширяться при дальнейшем развитии системы в целом.

Определение 1. Множество характеристических атрибутов X является подмножеством множества всех атрибутов A: $X \subset A$.

Определение 2. Тип функциональной обязанности задаётся набором пар характеристический атрибут — домен:

$$TFO := (X_1 : D_{x1}; ...; X_n : D_{xn}),$$

где $X_i \in$ X — характеристический атрибут, причём доменом характеристического атрибута X_i является субдомен домена соответствующего атрибута A_i: $D_{xi} \subseteq D_i$.

ТФО определяется на декартовом произведении доменов характеристических атрибутов $D_{x1} \times ... \times D_{xn}$.

Множество характеристических атрибутов является минимальным набором атрибутов, позволяющим описать все ТФО для данной модели.

Одной из основных проблем является введение такого описания характеристических атрибутов и функциональных обязанностей, исходя из которых можно было бы получить виртуальное отображение внешней модели пользователя БД — такие данные, на которые распространяются полномочия заданной ФО.

Определение 3. Функциональные обязанности задаются принадлежностью к определённому типу функциональных обязанностей и множеством конкретных значений характеристических атрибутов (M) — подмножеством декартового произведения доменов характеристических атрибутов:

$$FO := \langle TFO, M \rangle,$$

где $M \subset D_{x1} \times ... \times D_{xn}$;
или

$$FO := \left\langle TFO, \{(x_1, ..., x_n), x_i \in D_{xi}, i = \overline{1, n}\} \right\rangle.$$

Из утверждения 1 и определений 1–3 следует, что можно построить отображение БД, на которое будут распространяться полномочия ФО. Такое отображение будем называть **внешней моделью по ФО**. В частном случае такое отображение можно построить для конкретного отношения.

Для обозначения отображения по конкретному отношению и ФО будем использовать запись:

$$Ext_{FO}(R) : R \to R'.$$

В результате **преобразования** отношения R **к внешней модели по ФО** получается производное отношение R' с такой же схемой $Sch(R') = Sch(R)$ и

кортежами, удовлетворяющими условию на характеристических атрибутах ФО: значения атрибутов, соответствующих ХА, должны принадлежать множеству М. Если отношение R не содержит всех атрибутов, соответствующих определению данной ФО, для получения внешней модели берётся проекция по схеме отношения R от внешнего соединения отношений, содержащих ХА и связывающих их отношений. При построении запроса Q к БД (запрос к БД представляет собой функцию от отношений БД) для получения подмножества данных соответствующих ФО, от имени которой выполняется запрос, необходимо преобразовать запрос, возвращающий все возможные элементы, с помощью Ext:

$$Q = F\left(R_1, ..., R_m\right) \to Q' = F\left(R_1, ..., R_k, Ext_{FO}\left(R_{k+1}\right), ..., Ext_{FO}\left(R_m\right)\right).$$

Ext применяется к тем отношениям, на которые непосредственно распространяются права пользователя в данном запросе. Таким образом, запрос несёт в себе семантику описания доступа, но не содержит конкретных деталей реализации доступа: в запросе указывается только для каких отношений необходимо построить внешнюю модель.

Такой механизм может срабатывать в моделях, на схемы отношений которых наложены некоторые ограничения. Одним из таких ограничений является отсутствие так называемых «ветвлений» в схеме БД. Ветвление возникает при наличии нескольких путей в схеме БД от одного отношения к другому (наличие нескольких внешних ключей в отношении R_1, напрямую или посредством других отношений связывающих R_1 с R_2 связью $N:1$).

Пусть $TFO_1 = (X_1)$ — соответствует характеристическому атрибуту X_1, и в отношении R_2 существует два внешних ключа, связывающих R_2 с R_1 (рис. 1). Тогда встаёт вопрос об однозначности определения внешней модели отношения R_2, а именно, по какому предикату необходимо производить внешнее соединение между R_1 и R_2:

$$IdR_1 = FK_1 toR_1 \text{ или } IdR_1 = FK_2 toR_1 \text{ или } IdR_1 = FK_1 toR_1 \cap IdR_1 = FK_2 toR_1.$$

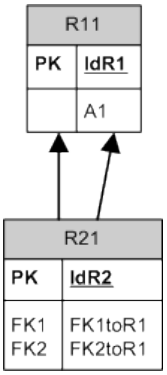

Рис. 1. **Два внешних ключа к одному отношению**

Аналогичная ситуация получается, когда R_1 и R_2 связаны не прямой связью, а через другие отношения (рис. 2) и существует несколько путей от R_2 к R_1.

Для учёта ветвлений в схеме БД в описании ТФО не хватает описания связей между отношениями – маршрутов, по которым должны работать ХА. Таким образом, необходимо в описании ТФО задавать некоторую структуру, отображающую не только набор ХА, но и наличие связей между отношениями, в которых они содержатся.

Предлагается задавать смысловые группы (связанных) отношений для ТФО, на которых должны работать ХА, т.е. ТФО — это не только набор выделенных

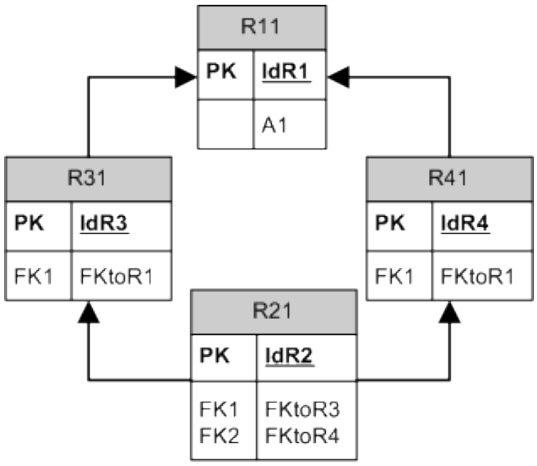

Рис. 2.

в схеме БД атрибутов, несущих смысловую нагрузку, но и их связи с другими отношениями — маршруты, по которым должны работать ХА при построении внешних моделей отношений.

Для описания связей будем использовать графы, построенные на основе схемы БД.

По схеме БД построим ориентированный граф G, в котором:
– вершины — это отношения базы данных,
– ребра — связи между отношениями.

Итак, граф, построенный на схеме БД, можно описать следующим образом:

$$G := (\mathrm{R}, \mathrm{L}),$$

где $\mathrm{R} = \{R_i\}$ — непустое множество отношений БД; L — множество связей между отношениями, причём:

$$\mathrm{L} = \{l_{ij_m}\},$$

где $l_{ij_m} = ((R_i, PK), (R_j, FK_m))$.

В схеме базы данных выделяются смысловые группы отношений (смысловые блоки) — группы отношений, задействованные в определённых контекстах использования (в логически связанных группах операций или процессов).

Определение 4. Смысловая группа отношений G_s — связный подграф графа G:

$$G_s = (\mathrm{R}_s, \mathrm{L}_s); \quad \mathrm{R}_s \subset \mathrm{R}, \quad \mathrm{L}_s \subset \mathrm{L}.$$

Введём уточнённое определение ТФО:

Определение 5. Типы функциональных обязанностей задаются набором характеристических атрибутов и смысловой группой отношений:

$$TFO := \langle (X_1 : D_{x1}; ...; X_n : D_{xn}), G_s \rangle,$$

где $X_i \in \mathrm{X}$ — характеристический атрибут, $G_s = (\mathrm{R}_s, \mathrm{L}_s) : X_i \in Sch[R_i]$, $R_i \in \mathrm{R}_s$.

Тогда построение внешней модели по ФО выражается следующей формулой:

Определение 6.

$$Ext_{FO}(R) = \pi_{Sch[R]} \left(\sigma_{(a_1,...,a_n) \in M} (G_s) \right),$$

где σ — оператор селекции, π — оператор проекции, $X_1, ..., X_n \in Sch\,[G_s]$ — a_k значение атрибута, соответствующего характеристическому атрибуту X_k .

При построении запроса к БД для получения подмножества данных соответствующих ФО, от имени которой выполняется запрос, происходит преобразование запроса с помощью Ext:

$$Q = F\,(R_1, ..., R_m) \to Q' = F\,(R_1, ..., Ext_{FO}\,(R_i)\,, ..., R_m)\,.$$

При использовании внешних моделей отношений по ФО значительно упрощается запись запросов. Облегчается реализация прав доступа. Разработчику необходимо только указать, для каких отношений необходимо использовать Ext — отношения, на которые в данном контексте непосредственно распространяются полномочия сотрудника. При подключении к системе пользователя с конкретной ФО отображение Ext достроит запрос и подставит значения ХА для данной ФО.

6. Заключение

В статье рассмотрен подход к организации разграничения доступа в информационных системах через построение виртуальных внешних моделей базы данных. Введены понятия функциональной обязанности, типа функциональной обязанности, характеристического атрибута, используемые для описания модели разграничения доступа. Предполагается, что рассмотренная модель значительно упростит механизм управления доступом к данным для рассматриваемого класса информационных систем.

Литература

1. *Гайдамакин Н. А.* Разграничение доступа к информации в компьютерных системах. — Екатеринбург: Издательство Уральского Университета, 2003. — 328 с. [*Gayjdamakin N. A.* Razgranichenie dostupa k informacii v kompjyuternihkh sistemakh. — Ekaterinburg: Izdateljstvo Uraljskogo Universiteta, 2003. — 328 s.]
2. *Девянин П. Н.* Модели безопасности компьютерных систем. — М.: Издательский центр «Академия», 2005. — 144 с. [*Devyanin P. N.* Modeli bezopasnosti kompjyuternihkh sistem. — M.: Izdateljskiyj centr "Akademiya 2005. — 144 s.]
3. *Sandhu R. S., Samarati P.* Access Control: Principles and Practice // IEEE Communications. — 1994. — No 32(9). — Pp. 40–48.
4. *Лепешкин О. М., Харечкин П. В.* Подходы к обеспечению функциональной применимости ролевой модели разграничения доступа в системе управления предприятия // Информационное противодействие угрозам терроризма. — 2008. — № 11. — С. 57–66. [*Lepeshkin O. M., Kharechkin P. V.* Podkhodih k obespecheniyu funkcionaljnoyj primenimosti rolevoyj modeli razgranicheniya dostupa v sisteme upravleniya predpriyatiya // Informacionnoe protivodeyjstvie ugrozam terrorizma. — 2008. — No 11. — S. 57–66.]
5. *Майоров А. В.* Улучшенная ролевая модель доступа к объектам. — `http://2008.secr.ru/en/etc/secr2008_andrey_mayorov_improved_role-based_access_control_model.pdf`. [*Mayjorov A. V.* Uluchshennaya rolevaya modelj dostupa k objhektam. — `http://2008.secr.ru/en/etc/secr2008_andrey_mayorov_improved_role-based_access_control_model.pdf`.]
6. *Griffiths P. G., Wade B.* An Authorization Mechanism for a Relational Database System // ACM TODS. — 1976. — Vol. 1, No 3. — Pp. 242–255.
7. *Polk W. T. L. E. B. I.* NIST Special Publication 800-8 Security Issues in the Database Language SQL. — 1993. — `http://craigchamberlain.com/library/security/NIST/NIST%20800-8%20-%20Security%20Issues%20in%20the%20Database%20Language%20SQL.pdf`.

8. *Bertino E., Jajodia S., Samarati P.* A Flexible Authorization Mechanism for Relational Data Management Systems // ACM Transactions on Information Systems (TOIS). — 1999. — Vol. 17, No 2. — Pp. 101–140.
9. *Date C. J.* A Formal Definition of the Relational Model // ACM SIGMOD Record. — 1982. — Vol. 13, No 1. — Pp. 18–29.
10. *Pirotte A.* A Precise Definition of Basic Relational Notions and of the Relational Algebra // ACM SIGMOD Record. — 1982. — Vol. 13, No 1. — Pp. 30–45.

UDC 004.65, 004.056

Data Access Control Via Virtual External Model

V. A. Petrov, O. D. Dolina, I. L. Tolmachev

Information Technology Department
Peoples' Friendship University of Russia
6, Miklukho–Maklaya str., Moscow, 117198, Russia

The article discusses the problem of organizing different levels of access to data within information systems. These are based on a relational database designed to automate the management of the enterprise. Here we introduce the necessary definitions and concepts to build a model that allows us to make the mechanism of restricting access to data at the level of the relational model.

Key words and phrases: data access control, access rights in information systems, access rights in relational database, virtual external model.