

Реляционная модель логического
разграничения доступа: теоретическое описание
и экспериментальная проверка
производительности

А. А. Иткес, К. А. Шапченко, В. Ю. Бухонов

НИИ механики МГУ, Мехмат МГУ

21 Октября 2014

План доклада

- ▶ Постановка задачи.
- ▶ Реляционная модель ЛРД – определение и свойства.
- ▶ Эксперименты по измерению производительности реализации модели.
- ▶ Планы дальнейшей работы над моделью.

Постановка задачи

Задача: Управление логическим разграничением доступа в многопользовательских сетевых информационных системах, включая ИАС «Наука-МГУ» (Истина).

- ▶ Множество пользователей системы постоянно меняется.
- ▶ Принадлежность объектов пользователям по схеме многие-ко-многим.
- ▶ Пользователи могут быть по-разному связаны с объектами.
- ▶ Права доступа пользователя к объекту зависят также от взаимосвязей объекта с другими объектами.

Реляционная модель ЛРД

В информационной системе заданы следующие множества:

- ▶ *Objects* – множество объектов;
- ▶ *Users* $\subset$ *Objects* – множество пользователей;
- ▶ *Classes* – множество классов;
- ▶ *Relations* – множество отношений;
- ▶ *Actions* – множество видов доступа.

Реляционная модель ЛРД на примере ИАС «Наука-МГУ» (Истина)

Классы объектов в ИАС «Наука-МГУ» (Истина):

- ▶ пользователь;
- ▶ сотрудник;
- ▶ результат научно-исследовательской деятельности;
- ▶ статья;
- ▶ журнал или сборник;
- ▶ организация или подразделение;
- ▶ ...

Реляционная модель ЛРД на примере ИАС «Наука-МГУ» (Истина)

Отношения между объектами в ИАС «Наука-МГУ» (Истина):

- ▶ пользователь соответствует сотруднику;
- ▶ сотрудник является автором статьи;
- ▶ статья опубликована в журнале;
- ▶ сотрудник работает в подразделении;
- ▶ пользователь является ответственным по подразделению;
- ▶ одно подразделение входит в другое;
- ▶ ...

Реляционная модель ЛРД на примере ИАС «Наука-МГУ» (Истина)

Виды доступа к объекту «статья» в ИАС «Наука-МГУ»
(Истина):

- ▶ изменить привязку к авторам;
- ▶ изменить привязку к журналу;
- ▶ изменить название;
- ▶ загрузить полный текст;
- ▶ скачать полный текст;
- ▶ ...

Реляционная модель ЛРД

Также в информационной системе заданы следующие отношения:

- ▶ $ObjectsRelations \subset Objects \times Relations \times Objects$;
- ▶ $RelationAccessGranted \subset Relations \times Actions$;
- ▶ $ClassActions \subset Classes \times Actions$;
- ▶ $RelationLeftClass : Relations \rightarrow Classes$;
- ▶ $RelationRightClass : Relations \rightarrow Classes$;
- ▶ $RelationTransitions \subset Relations \times Relations \times Relations$.

Реляционная модель ЛРД

- ▶ $ObjectRelations_0 = ObjectRelations$;
- ▶ $ObjectRelations_{n+1} = \{(o_1, r_{13}, o_3) :$
 $(o_1, r_{12}, o_2), (o_2, r_{23}, o_3) \in ObjectRelations_n, (r_{12}, r_{23}, r_{13}) \in$
 $RelationTransitions\}$;
- ▶ $\overline{ObjectRelations} = \bigcup_{n=0}^{\infty} ObjectRelations_n$.

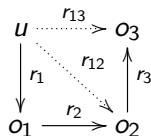
Пользователь u имеет право доступа a к объекту o , если существует такое отношение r , что $(u, r, o) \in \overline{ObjectRelations}$ и $(r, a) \in RelationAccessGranted$.

Доступ к объектам по цепочке отношений

- ▶ Пользователь u связан отношением r_1 с объектом o_1 ;
- ▶ объект o_1 связан отношением r_2 с объектом o_2 ;
- ▶ объект o_2 связан отношением r_3 с объектом o_3 ;
- ▶ есть правило переноса отношений $(r_1, r_2) \rightarrow r_{12}$;
- ▶ есть правило переноса отношений $(r_{12}, r_3) \rightarrow r_{13}$;
- ▶ отношение r_{13} дает пользователю право доступа a к объектам.

Тогда пользователь u имеет право доступа a к объекту o_3 по цепочке (r_1, r_2, r_3) , порождающей отношение r_{13} .

Доступ к объектам по цепочке отношений



Пользователь u имеет право доступа а к объекту o_3 по цепочке (r_1, r_2, r_3) , порождающей отношение r_{13} .

Доступ к объектам по цепочке отношений на примере ИАС «Наука-МГУ» (Истина)

Доступ к объектам по цепочке отношений:

- ▶ Пользователь A является ответственным по подразделению B ;
- ▶ подразделение C входит в подразделение B ;
- ▶ сотрудник D работает в подразделении C ;
- ▶ сотрудник D является автором статьи E .

Пользователь A имеет некоторые права доступа к статье E по цепочке объектов A, B, C, D, E .

Теоретическая оценка производительности механизмов реляционной модели ЛРД

Задача: оценить максимальную длину цепочки отношений в системе.

Если ни одно из отношений в системе не может быть порождено цепочкой, содержащей его само, то максимальная длина цепочки отношений не превосходит $2^{\|Relations\| - 1}$.

Эксперименты по измерению производительности механизмов реляционной модели ЛРД

Алгоритм работы функции проверки доступа – получить список разрешенных видов доступа пользователя u к объекту o класса c .

- ▶ Установить $allowed = \emptyset$.
- ▶ для каждой цепочки отношений, которая может связывать пользователя с объектом класса c выполнить:
 - ▶ с помощью SQL-запроса проверить, существует ли цепочка объектов, по которой пользователь u связан с объектом o данной цепочкой отношений;
 - ▶ если она существует, то добавить в $allowed$ виды доступа, соответствующие отношению, порождаемому данной цепочкой;
- ▶ вернуть ($allowed$).

Эксперименты по измерению производительности механизмов реляционной модели ЛРД

Количество объектов ИАС «Наука-МГУ» (Истина) в июне 2014:

- ▶ пользователи – около 10000;
- ▶ сотрудники – около 100000;
- ▶ статьи – около 200000;
- ▶ связок статьи с автором – около 1000000.

Эксперименты по измерению производительности механизмов реляционной модели ЛРД

Объекты в тестовой базе данных:

- ▶ пользователи – 100000;
- ▶ сотрудники – 100000;
- ▶ статьи – 200000;
- ▶ подразделения – 5000;
- ▶ журналы – 5000.

Эксперименты по измерению производительности механизмов реляционной модели ЛРД

Отношения в тестовой базе данных:

- ▶ каждый сотрудник соответствует единственному пользователю а каждый пользователь – единственному сотруднику;
- ▶ вероятность того, что случайно выбранный пользователь является автором случайно выбранной статьи – 0.00005;
- ▶ вероятность того, что случайно выбранный пользователь является ответственным по случайно выбранному подразделению – 0.0001;
- ▶ вероятность того, что случайно выбранный сотрудник работает в случайно выбранном подразделении – 0.001.

Эксперименты по измерению производительности механизмов реляционной модели ЛРД

Правила переноса отношений:

- ▶ если пользователь связан с сотрудником, и сотрудник является автором статьи, то пользователь является автором статьи;
- ▶ если пользователь – ответственный по подразделению и сотрудник работает в подразделении, то пользователь является ответственным по месту работы сотрудника;
- ▶ если пользователь является ответственным по месту работы сотрудника и сотрудник является автором статьи, то пользователь является ответственным по месту написания статьи.

Время получения списка допустимых операций с данным объектом для данного пользователя – от 1 до 3 миллисекунд.

Планы дальнейшей работы над моделью

- ▶ Использование модели при наличии в системе транзитивных отношений.
- ▶ Объединение с ролевой моделью ЛРД.
- ▶ Ввод объекта «сеанс доступа к системе».