Модели логического разграничения доступа ABAC, EBAC и ChRelBAC: описание и сравнительный анализ с точки зрения применения в многопользовательских системах управления наукометрическим контентом

В. Ю. Бухонов, А. А. Иткес

Мех.-мат. МГУ, НИИ механики МГУ

15 ноября 2016

План доклада

- Управление доступом к данным в информационно-аналитической системе (ИАС) «ИСТИНА».
- Определение реляционной модели логического разграничения доступа (ЛРД).
- Сравнение с моделями ABAC и EBAC.
- Программная реализация реляционной модели ЛРД.
- Планы дальнейшей работы над реляционной моделью ЛРД.

Управление доступом к данным в ИАС «ИСТИНА»

- Множество пользователей динамически изменяется без участия администратора.
- Большое количество разновидностей объектов и видов взаимосвязей между ними.
- Высокая скорость изменения множеств объектов и отношений между ними разными пользователями.
- Многие объекты не имеют пользователя-владельца.

Требования к механизмам разграничения доступа к данным ИАС «ИСТИНА»

- Предлагается использовать модель, основанную на представлении системы в виде графа.
- Модель должна учитывать отношения как между пользователями, так и между ресурсами системы.
- Модель должна учитывать не только топологические свойства социального графа, но и дополнительные свойства объектов и отношений между ними.

Модели разграничения доступа в социальных сетях

- Модели Фонга
- Модели Карминати-Феррари
- Модели Ченга, Парка и Сандху
- Attribute-Based Access Control
- Entity-Based Access Control

Реляционная модель логического разграничения доступа

Пусть в системе заданы следующие множества:

- *Objects* – множество объектов;
- *Users* $\subset$ *Objects* – множество пользователей;
- *Classes* – множество классов;
- *Actions* – множество возможных операций над объектами;
- *Relations* – множество [имен] отношений;
- *Chains* - множество цепочек отношений;

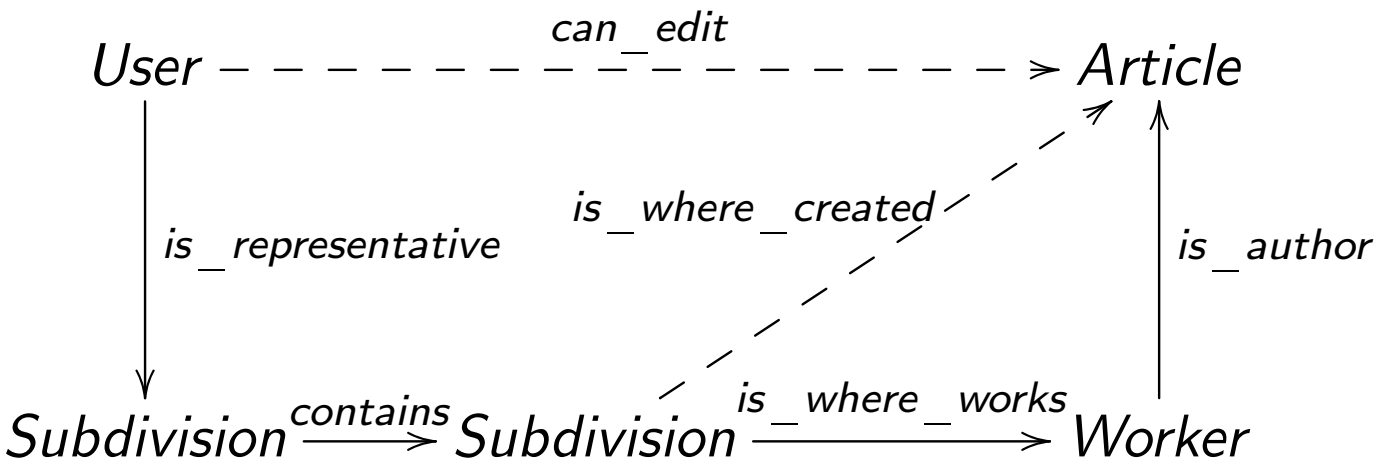
Цепочка отношений $chain = ((r_1, \ldots, r_n), r_{prod}, cond)$.

Реляционная модель логического разграничения доступа

Пусть в системе заданы следующие отношения:

- $ObjectRelations \subset Objects \times Relations \times Objects$ – определяет, какие пары объектов связаны тем или иным отношением;
- $RelationAccessGranted \subset Relations \times Actions$, определяющее, какие виды доступа разрешены для пользователя к объекту, связанному с ним определенным отношением;
- $RelationAccessDenied \subset Relations \times Actions$, определяющее, какие виды доступа запрещены для пользователя к объекту, связанному с ним определенным отношением.

Пример цепочки отношений



Реляционная модель логического разграничения доступа

Пусть также для некоторых классов и отношений в системе задано множество атрибутов.

- Атрибут класса c – это тройка $(name, possibleValues, f)$, где $name$ – имя атрибута, $possibleValues$ – область значений атрибута, $f : \{o \in Objects : class(o) \leq c\} \to possibleValues$;
- Атрибут отношения r – это тройка $(name, possibleValues, f)$, где $name$ – имя атрибута, $possibleValues$ – область значений атрибута, $f : \{(o_1, o_2) : (o_1, r, o_2) \in ObjectRelations\} \to values$;
- Для класса c общее множество значений атрибутов $AttributeValues(c) = \prod_{a \in Attributes(c)} possibleValues(a)$;
- Для отношения r общее множество значений атрибутов $AttributeValues(c) = \prod_{a \in Attributes(r)} possibleValues(a)$.

Реляционная модель логического разграничения доступа

Пусть также в системе используются переменные окружения, представляющие собой атрибуты, не ассоциированные ни с каким конкретным объектом.

- *EnvironmentKeys* – множество переменных окружения, которые не являются объектами, но их значения могут влиять на права доступа к объектам.
- *EnvironmentValues* – множество значений переменных окружения в данный момент.

Реляционная модель логического разграничения доступа

Значение о предоставлении пользователю доступа к объекту может зависеть от значений атрибутов пользователя, целевого объекта и переменных окружения. Для этого в системе также заданы отношения.

- $RelationAccessGranted_P \subset Relations \times Actions$, определяющее, какие виды доступа разрешены для пользователя к объекту, связанному с ним определенным отношением;
- $RelationAccessDenied_P \subset Relations \times Actions$, определяющее, какие виды доступа запрещены для пользователя к объекту, связанному с ним определенным отношением.

Здесь $P : EnvironmentValues \times AttributeValues(user) \times AttributeValues(object) \to \{true, false\}$. Разрешение или запрет на предоставление пользователю доступа к объекту действует только в том случае, если $P(environment, user, object) = true$.

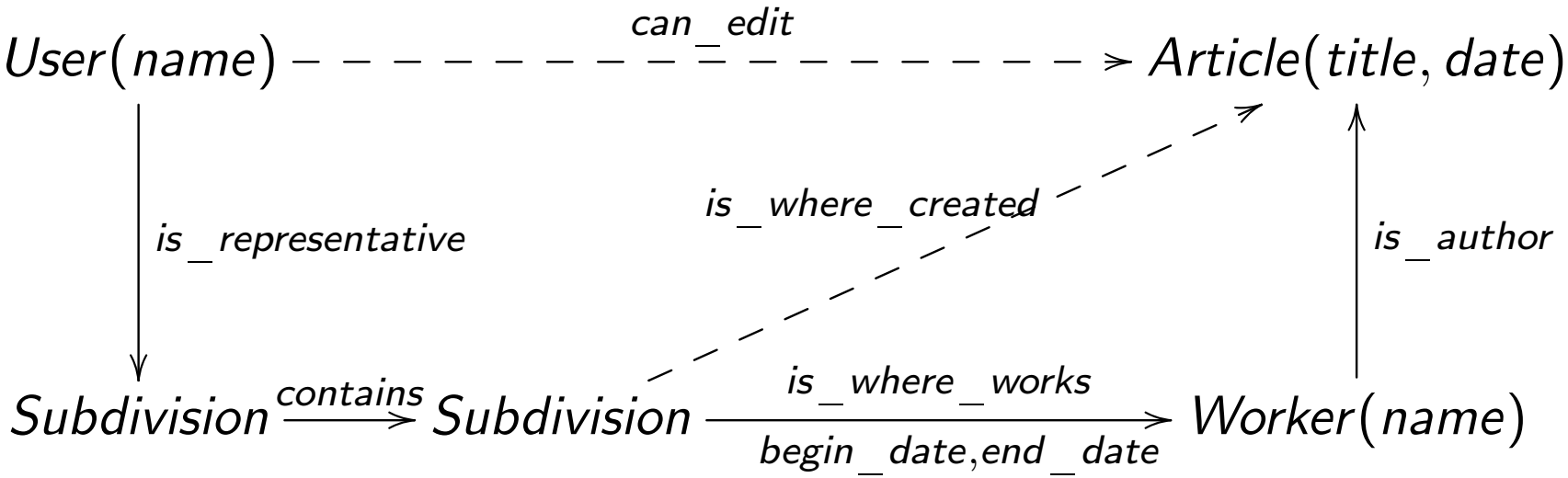
Цепочка отношений

Цепочка отношений $chain = ((r_1, \ldots, r_n), r_{prod}, cond)$, где
$cond : (o_0, \ldots, o_n) \to \{true, false\}$.
Условие соединения объектов o_0 и o_n отношением, порожденным цепочкой, называемое цепным предикатом.

$$CP_0(o_0, o_n) = \exists o_1, \ldots, o_{n-1} : r_1(o_0, o_1) \wedge \ldots \wedge r_n(o_{n-1}, o_n) \wedge P(o_1, \ldots, o_n).$$

Где P – бескванторная формула, представляющая собой условие цепочки.

Пример цепочки отношений



Условие цепочки:

$Article.date \geq is\_where\_works.begin\_date \wedge (Article.date \leq is\_where\_works.end\_date \vee isNull(is\_where\_works.end\_date))$.

Использование кванторов всеобщности

Цепным предикатом называется

$$CP_0(o_0, o_n) = \exists o_1, \ldots, o_{n-1} : r_1(o_0, o_1) \wedge \ldots \wedge r_n(o_{n-1}, o_n) \wedge P(o_1, \ldots, o_n).$$

Расширенным цепным предикатом первого уровня называется

$$CP_1(u, o) = \exists o' : (P(u, o') \wedge Q(o', o)) \wedge \forall o' : (Q(o', o) \rightarrow P(u, o')).$$

Где P и Q – цепные предикаты.

Свойства корректности реляционной модели

Условия корректности реляционной модели ЛРД

- Отсутствие циклических зависимостей атрибутов.
- Отсутствие циклических зависимостей отношений.

Модель Attribute-Based Access Control

- Предоставление пользователю доступа к объекту зависит от:
  - атрибутов пользователя;
  - атрибутов целевого объекта;
  - переменных окружения.
- Цепочки отношений не поддерживаются.

Модель Entity-Based Access Control

- Предоставление пользователю доступа к объекту зависит от:
  - атрибутов пользователя и объектов, связанных с ним определенным отношением;
  - атрибутов целевого объекта и объектов, связанных с ним определенным отношением;
  - атрибутов целевого действия;
  - переменных окружения.
- Атрибуты отношений не поддерживаются.
- Вспомогательные цепочки отношений не поддерживаются.
- Отсутствуют математически строгие определения и формулировки.

Требования к программной реализации

- Автоматизированная проверка свойств корректности модели перед любым изменением правил, к которым непосредственно обращается WEB-приложение.
- Отсутствие необходимости в модификации алгоритма проверки прав доступа при каждом изменении правил модели.
- Приемлемая производительность механизмов разграничения доступа для системы, в которой одновременно работают сотни пользователей.

Программная реализация

- Разработан программный комплекс, создающий функцию проверки прав доступа пользователя к объекту на основании описания модели.
- Функция принимает на входе идентификатор пользователя, класс и идентификатор целевого объекта и возвращает список разрешенных видов доступа этого пользователя к этому объекту.
- Создаваемая функция не содержит циклов, рекурсий и переходов на более ранние инструкции, и поэтому гарантирована от зацикливания.
- Все запросы к базе данных жестко закодированы в создаваемой функции, за исключением необходимости в подстановке значений идентификатора пользователя, объекта и переменных окружения.

Алгоритм создания функции проверки прав доступа

- Приведение множества цепочек к каноническому виду.
- Удаление цепочек, первый объект которых не является пользователем.
- Преобразование оставшихся цепочек в шаблоны SQL-запросов.

Дальнейшее развитие модели

- Введение других активных сущностей, кроме пользователей – например, сеансов доступа.
- Учет множественных действий с объектами.
- Анализ динамики изменений модели во времени.

Объект множественного действия

Множественное действие $ma(o_1, \ldots, o_n)$ включает в себя

- $Actions_i$ – действия, выполняемые над объектом o_i;
- $(o_i, r_{ij}^{required}, o_j)$ – необходимые отношения;
- $(o_i, r_{ij}^{blocking}, o_j)$ – блокирующие отношения;
- $(o_i, r_{ij}^{eastablished}, o_j)$ – отношения, которые будут установлены;
- $(o_i, r_{ij}^{broken}, o_j)$ – отношения, которые будут разорваны.

Объект множественного действия

Множественное действие – изменение одного из авторов публикации.

- $o_1 = old\_author$ – прежний автор;
- $o_2 = article$ – статья;
- $o_3 = new\_author$ – новый автор;
- $Actions_1 = disconnectArticle$;
- $Actions_2 = changeAuthor$;
- $Actions_3 = connectArticle$;

Объект множественного действия

Множественное действие – изменение одного из авторов публикации.

- $requiredRelations = (old\_author, isAuthor, article)$;
- $blockingRelations = (new\_author, isAuthor, article)$;
- $eastablishedRelations = (new\_author, isAuthor, article)$;
- $brokenRelations = (old\_author, isAuthor, article)$.

Литература

Васенин В. А., Иткес А. А., Шапченко К. А., Бухонов В. Ю. Реляционная модель логического разграничения доступа на основе цепочек отношений / Программная инженерия, № 9, 2015 г. — М.: «Новые технологии», 2015. — С. 11-19.

J. Bogaerts, M. Decat, B. Lagaisse, W. Joosen. Entity-Based Access Control: supporting more expressive access control policies / «ACSAC 2015 Proceedings of the 31st Annual Computer Security Applications Conference», 2015 — С. 291 – 300.

V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone. NIST Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, 2014. — 37 С.

Васенин В. А., Иткес А. А., Шапченко К. А. О применении моделей разграничения доступа в социальных сетях к одному классу многопользовательских систем управления контентом. / Программная инженерия, № 4, 2015 г. — М.: «Новые технологии», 2015. — С. 10-19.