УДК 004.415
ББК 32.973.202-018.2

МНОГОУРОВНЕВАЯ БЕЗОПАСНОСТЬ ДЛЯ СЕМАНТИЧЕСКИХ ДАННЫХ

Хоанг Ван Кует
(Национальный Исследовательский Томский Политехнический Университет)

Безопасность семантических данных будем обеспечивать с помощью многоуровневой безопасностью. Рассматривается простой алгоритм метода поддержки работы с онтологическими данными. Рассмотрены два вида безопасности семантических данных: произвольная и многоуровневая, которая имеет большую эффективность по сравнению с произвольной безопасностью. Для определения многоуровневой классификации данных использованы характеристики языка описания ресурсов и онтологий. Приведены логические выводы для построения многоуровневой безопасности.

Ключевые слова: многоуровневая безопасность, язык описания ресурсов (RDF), язык описания онтологии (OWL), доступ к данным, семантические данные.

1. Введение

Одной из важнейших задач при разработке СИС является безопасность работы семантических баз данных. Для её решения необходимо выполнить следующие этапы: создать алгоритм для поддержки безопасности работы с семантическими данными, контролировать доступ к данным, обеспечить безопасность RDF и OWL документов и логический вывод для них.

Одной из самых важных задач для обеспечения многоуровневой безопасности данных является разделение прав

доступа пользователей к этим данным и определение уровней политики доступа к каждой части документов, хранимых в семантической базе данных. Эти задачи могут быть решены с помощью многоуровневой безопасности.

Целью данной статьи является описание построения многоуровневой безопасности, обеспечивающей работу с семантическими данными. Для достижения поставленной цели рассматривается произвольная безопасность для базы данных, предлагается общий алгоритм обеспечения многоуровневой безопасности данных, исследуется метод построения многоуровневой безопасности для управления семантическими данными и приводится логический вывод многоуровневой безопасности онтологических данных.

2. Безопасность для баз данных

2.1. ПРОИЗВОЛЬНАЯ БЕЗОПАСНОСТЬ

Произвольная безопасность касается доступа к данным в зависимости от пользователей, групп пользователей, а также других факторов, таких как роли пользователей. Произвольная безопасность включает в себя 3 компоненты: контроль доступа и авторизации политики, администрирование политик, идентификацию и аутентификацию политики [1]. При произвольной безопасности все данные в базе данных будут безопасными, но иногда какая-то часть данных нужна для использования в каких–то операциях, к которым у пользователей нет доступа. Поэтому произвольная безопасность не обладает гибкостью.

Для повышения безопасности семантических баз данных безопасность должна выполняться на всех уровнях прав использования данных пользователями [8]. Тогда каждый пользователь будет получать собственные права доступа к конкретным частям базы данных. Для этого, необходимо осуществляется многоуровневая безопасность данных.

2.2. МНОГОУРОВНЕВАЯ БЕЗОПАСНОСТЬ БАЗЫ ДАННЫХ

Многочисленные сообщения о многоуровневой безопасности системы управления базами данных поступали на протяжении 1980-х и в начале 1990-х г.г. Эти системы эволюционировали от многоуровневых защищенных операционных систем. Раннее развитие сосредоточено на многоуровневой безопасности реляционных баз данных. Затем внимание было уделено многоуровневой системе управления базами данных объекта и многоуровневых распределенных систем баз данных. Многоуровневое безопасное управление данными включает в себя многоуровневую безопасность политики, многоуровневую модель данных и многоуровневую базу данных управления функциями [7].

Доступ к данным пользователям будет предоставлен в зависимости от оформления уровня их прав и уровня чувствительности данных [6]. Данные могут быть указаны в разных уровнях классификаций, таких как: неклассифицированных, конфиденциальных, секретных и сверхсекретных.

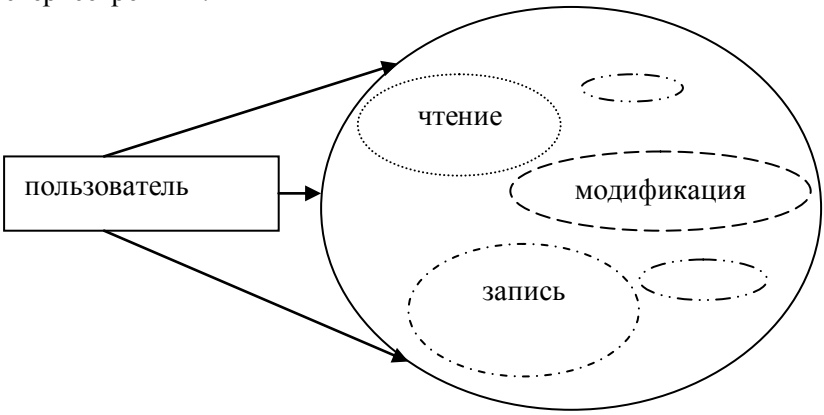

Рис. 1. Права доступа пользователей к данным

К неклассифицированному уровню все пользователя имеют доступ, но к конфиденциальному уровню не все пользователя имеют права доступа. К секретному и сверхсекретному уровням

только некоторые пользователи имеют доступ [3]. Они также имеют разные права доступа к данным, находящимся в конфиденциальной, секретной и сверхсекретной уровнях. Они могут читать, писать, изменить и выполнить какие-то операции с данными. На рис. 1 представлены разные права доступа пользователя. Пользователь имеет доступ к данным, но к разным частям данных его права могут быть разными.

3. Построение многоуровневой безопасности для семантических баз данных

3.1. АЛГОРИТМ РАБОТЫ ПОДПРОГРАМЫ ОБЕСПЕЧЕНИЯ РАБОТЫ С СЕМАНТИЧЕСКИМИ ДАННЫМИ

Основные требования по безопасности онтологических данных во многом совпадают с требованиями, предъявляемыми к безопасности реляционных данных: контроль доступа, криптозащита, проверка целостности, протоколирование. Но для безопасности онтологических данных, которые зависят от характеристик и особенностей языков RDF и OWL, необходимы дополнительные требования: определение политики доступа пользователей, многоуровневая безопасность данных, т.е. определение существования данных, определение классификации политик доступа к частям данных, определение прав доступ пользователей к данным.

На рис. 2 приведён алгоритм работы подпрограммы поддержки работы с онтологическими данными с помощью использования многоуровневой безопасности.

По этому алгоритму неавторизованный пользователь не имеет права доступа к онтологическим данным. Авторизованный пользователь имеет доступ к онтологическим данным. В зависимости от должности пользователей их право доступа к данным является разным: одни могут только читать данные, а другие - изменять, добавлять и удалять данные.

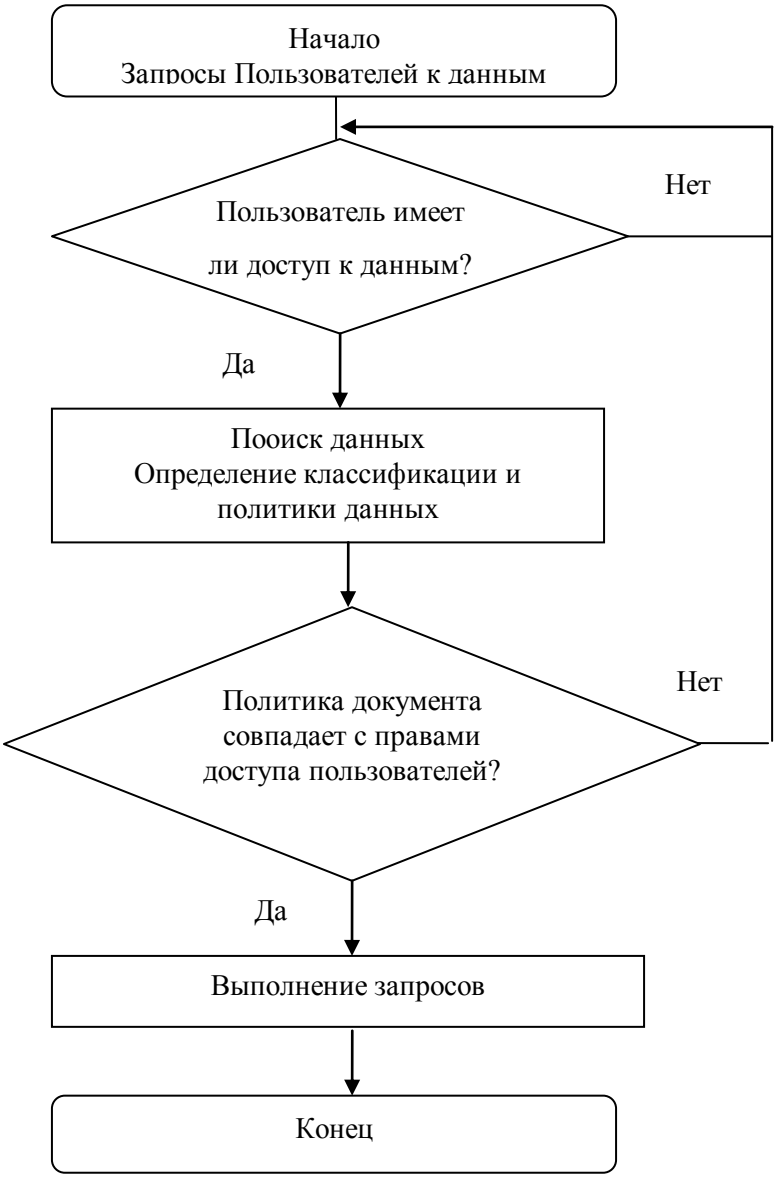

Рис. 2. Алгоритм для обеспечения работы с онтологическими данными

Если пользователь отправляет запросы к данным, имея право доступа к ним, то подпрограмма будет выполнять последовательные операции, такие как: поиск данных, определение классификации политик данных. Если у пользователя отсутствует право доступа к данным, то он не может отправлять запросы к данным. После выполнения последовательных операций, подпрограмма проверяет соответствие между классификациями политик частей данных и прав пользователей на чтение, изменение данных. Если они совпадают, то запрос выполняется, если нет, то пользователь должен отправить другой запрос к данным.

Многоуровневая безопасность эффективнее, чем произвольная безопасность, так как она позволяет определять права пользователей по доступу к различным частям БД, вплоть до конкретного элемента. При этом имеется возможность не только предоставить доступ тому или иному пользователю, но и указать разрешенный тип доступа: что именно может делать конкретный пользователь с конкретными данными (читать, модифицировать, удалять и т.д.).

3.2. МНОГОУРОВНЕВАЯ БЕЗОПАСНОСТЬ RDF-ДОКУМЕНТОВ

Основными компонентами семантической базы данных являются RDF и OWL документы [9]. Для выполнения многоуровневой безопасности на семантических данных необходимо осуществить безопасность на разных уровнях RDF и OWL документов.

Язык RDF является основным языком описания семантических данных. Он позволяет описать содержание документов и отношение между различными их разделами [4]. Использование языка RDF обеспечивает улучшение взаимодействия между данными, повышает качество выполнения поиска и категоризации данных. С помощью языка RDF можно указать политику доступа пользователей к каждой части данных по уровням их классификации, которые приведены на рис. 3.

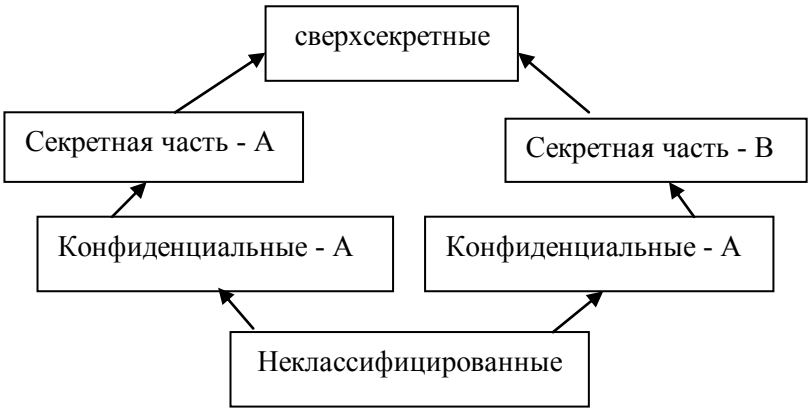

Рис. 3. Уровни классификации данных

Для выполнения многоуровневой безопасности доступа к RDF документам необходимо решить следующие задачи:

1. Классифицировать RDF данные во всех документах или только в некоторых частях;
2. Определить политику безопасности для прав доступа пользователей к RDF документам и их частям;
3. Применить принципы обеспечения безопасности реляционных данных к RDF данным;
4. Применить политики безопасности в схеме RDF данных;
5. Исполнить правила в отношении содержания, контекста и динамической безопасности;
6. Обеспечить многоуровневую безопасность к запросам на изменения и процесса обмена данными для баз RDF данных [8];
7. Обеспечить логический результат, получаемый пользователем на выходе, совершенно точным и обладающим полной структурой RDF представления: субъект - свойства - объекты.

3.3. МНОГОУРОВНЕВАЯ БЕЗОПАСНОСТЬ OWL-ДОКУМЕНТОВ

Язык OWL является более выразительным и имеет возможность выполнения логического вывода больше, чем RDF-язык**.** Для выполнения многоуровневой безопасности OWL-

документов необходимо решить все вышеперечисленные задачи для обеспечения безопасности RDF- документов, а также выполнить дополнительные задачи:

1. Использовать особенности RDF- схемы в OWL- языке для определения многоуровневой политики. Например, элементы: `rdfs:domain, rdfs:range` можно использовать для определения домена и диапазона данных, к которым пользователи имеют доступ;
2. Использовать характеристики свойств OWL- языка для определения прав доступ пользователей к данным, а также классификацию уровней политики данных. Например, для указания прав доступа пользователей можно использовать: симметричное свойство (`symmetricProperty`), обратно-функциональное свойство (`inverseFunctionalProperty`), транзитивное свойство (`transitiveProperty`);
3. Использовать ограничения свойств в языке OWL для определения права доступ пользователей к разным частям данных, например: `allValuesFrom, someValuesFrom`;
4. Использовать ограниченные кардинальности в языке OWL для указания количества классов пользователей, имеющих доступ к конкретным данным, например: `maxCardinality, cardinality minCardinality`. Если минимальная кардинальность `minCardinality=1`, то любой представитель этого класса будет связан по этому свойству по крайней мере с одним индивидом пользователей.

Вывод

Многоуровневая безопасность для семантических данных играет важную роль в процессе управления семантическими данными информационных систем. Она позволяет проверять права доступа каждого пользователя и четко определить, какие части данных могут быть доступы разным группам пользователей. Пользователи могут читать, заносить и изменять данные. Одни и те же данные могут являться доступными для одних пользователей, но секретными для других пользователей.

Благодаря разделению данных на разных уровнях доступа, степень обеспечения данных увеличивается, а это означает, что данные становятся более безопасными. Основными элементами семантических баз данных являются RDF и OWL данные, поэтому для решения задачи построения многоуровневой безопасности семантических данных необходимо создать многоуровневую систему безопасности для RDF и OWL документов.

В данной статье определены основные задачи для решения поставленной проблемы, показаны способ классификации уровней доступа к частям документа и метод использования языков RDF и OWL для определения прав доступа пользователей. Приведены примеры по использованию RDF и OWL для создания политик доступа пользователей. Был рассмотрен логический вывод в многоуровневой безопасности онтологических данных, правильность которого зависит от метода использования OWL и RDF для решения логического отношения между данными.

Литература

1. B. Thuraisingha, *Database and Applications Security: Integrating Data Management and Information Security*, CRC Press, Boca Raton, FL, 2005.
2. B. Thuraisingham, *Secure Sematic web Services*, Technical Report, University of Texas – Department of Computer Science, 2007.
3. B.Thuraisingham, Security for the semantic web, Computer Standards and Interfaces 27, 257 – 268, 2005.
4. Dean Allemang. *Semantic Web for the working ontologist : effective modeling in RDFS and OWL* / Dean Allemang, Jim Hendler. – 2nd ed. p. cm, 2011.
5. E. Bertino, et al., *Access Control for XML Documents, Data and Knowledge Engineering*, North Holland, 2002, pp. 237–260.
6. P. Reddivari, T. Finin, and A. Joshi. *Policy based Access Control for a RDF Store. In Proceedings of the Policy Management*

for the Web Workshop, A WWW 2005 Workshop, pages 78–83. W3C, May 2005.
7. P. Stachour and B. Thuraisingham. Design of LDV: *A multilevel secure relational database management system*. IEEE Trans. Knowledge and Data Eng.,2(2):190–209, June 1990.
8. R. Sandhu, E. J. Coyne, H. Feinstein, and C. Youman. *Role-based access control models*. IEEE Computer, 29(2):38–47, February 1996.
9. *Resource Description Framework* // [Электронный ресурс]. – 2006. – Режим доступа: [http://www.aot.ru/technology.html].

MULTILEVEL SECURITY FOR SEMANTIC DATA

Hoang Van Quyet: National Research Tomsk Polytechnic University, postgraduate (student8050@sibmail.com).

Abstract: semantic data will be securitized by using multi-level security. A simple algorithm method for supporting the work of ontological data is considered. Two types of semantic security of data are examined: random and multi-level security, which has a higher efficiency compared to any security. The characteristics of resources description language and ontology web language are used for determining the classification of multi-level data.

Keywords: multilevel security, resource description framework (RDF), ontology Web language (OWL), specifies policy, access to data.