OLAP 상에서 효율적인 정보 보호를 위한 데이터 접근 제어 방법

민병국, 최옥경, 예홍진
아주대학교 대학원 지식정보보안학과
e-mail : bkmin@ajou.ac.kr, okchoi@ajou.ac.kr, hjyeh@ajou.ac.kr

Data Access Control Method for The Efficient Information Security on OLAP

Byoung-Kuk Min, Okkyung Choi, Hong-Jin Yeh
Dept. of Knowledge Information Security, Graduate School of Ajou University

요 약

OLAP(On-Line Analytical Processing) 툴은 조직 운영에서 발생하는 데이터의 양이 많아짐에 따라 분석 수요도 함께 급증하며 전문 분석가의 역량만으로는 처리할 수 없는 분석 요구 사항을 충족시키기 위한 툴이다. OLAP 에서는 다양한 사용자가 직접 데이터베이스에 접근하여 대화식으로 질의를 던지고 응답을 받아 분석 업무를 진행할 수 있다. 이렇게 많은 사용자들이 데이터베이스에 직접 접근을 하게 됨에 따라 조직의 민감한 데이터를 지키기 위한 보안 정책이 필수가 되었다. 하지만 기존 연구에서는 OLAP 의 기능적인 분석에 치중하여 MDX(Multidimensional Expressions)와 XMLA(XML for Analysis) 등의 기법으로 기능을 구현하는 것에 그치고 있다. 이에 본 연구에서는 OLAP 보안 관련 연구를 분석하고 보안 모듈을 설계하여 효율적인 정보 보호를 위한 데이터 접근 제어 방법을 제시한다.

1. 서론

IT 기술의 발전과 더불어 각 조직에 쌓이는 데이터의 양도 함께 증가하고 있다. 이러한 데이터는 분석을 통해 조직이 다년간 걸어온 길과 걸어갈 길을 보여 주기도 한다. 초기의 조직들은 IT 전문가를 통해 조직의 데이터를 분석하고 보고서를 작성하여 조직의 의사 결정에 활용하였지만, 점점 늘어나는 데이터에 대한 분석 수요를 감당하기 어려워졌다.

OLAP 은 다양한 사용자의 데이터 분석 수요를 충족시키기 위해 사용자가 직접 조직의 데이터베이스에 접근하도록 지원한다. 이렇게 구축된 OLAP 시스템은 고객관계관리(CRM), 경영정보시스템(MIS) 등에 이용된다. 이전에 IT 전문가를 통해서 분석을 수행할 때보다 더욱 빠른 응답 시간과 요청 분석에 대한 정확성을 획기적으로 보장할 수 있다.

OLAP 은 조직의 의사 결정에 소비되는 시간을 획기적으로 줄여 주고 다양한 사용자에게 분석 업무가 가능하도록 도와 주었지만, 한 편으로는 조직의 데이터베이스에 대한 접근이 누구에게나 허용되면서 정보 접근을 제어할 보안 대책이 필요하게 되었다.

본 논문에서는 기존 논문에서 다루었던 OLAP 보안에 대한 이슈들을 분석하고, 특히 효율적인 정보 보호 정책이 수립될 수 있도록 접근 대상을 기능, 컨텐츠, 큐브데이터로 분류하고, RBAC(Role Based Access Control), Filtering SQL 기법을 사용하여 데이터 접근 제어를 제안하고자 한다.

2. 관련 연구

이 장에서는 본 논문에서 제안하는 OLAP 상에서의 데이터 접근 제어를 위해 OLAP 과 데이터마이닝 그리고 국내에서는 거의 이루어지지 않는 OLAP 보안 관련 연구에 대해서 설명한다.

2.1. OLAP 과 데이터마이닝

2.1.1. OLAP

OLAP 은 DW(Data Warehouse) 또는 특화된 DM(Data Mart)로부터 지식을 추출하여 의사 결정을 지원하는 시스템을 뜻한다. 주요 목적은 비전문가에게, IT 전문가의 개입 없이도, 데이터에 직접 접근하여 대화식으로 Ad-Hoc 쿼리를 만들도록 하는 것이다.

OLAP 은 큐브 데이터에 Slice, Dice, Drill-Down, Rollup 등의 기본 연산을 수행하여 최종적으로 피벗 분석을 통해 다차원 분석이 가능하도록 한다. 분석된 데이터를 통해 조직의 현황을 파악하고 의사 결정을 돕는 역할을 한다. 최근에는 예상 데이터를 이용한 시뮬레이션 분석을 통해 앞으로 다가올 시장을 내다보기도 한다[1]. OLTP(On-Line Transactional Processing)에 대조적으로 도입되어 서로 다른 요구 사항과 특징을 반영한다.

다음 <표 1>에서는 OLAP 과 OLTP 의 단적인 비교를 보여주고 있다[2].

<표 1> OLAP 과 OLTP 의 비교[2]

	OLTP	OLAP
Usage	Application specific	Decision support
Workload	Predefined	Unforeseeable
Access	Read/Write	Read-Only
Query structure	Simple	Complex
Records per operation	Tens/Hundreds	Thousands/Millions
Number of users	Thousands/Millions	Tens/Hundreds

2.1.2. 데이터마이닝

데이터마이닝(data mining)은 대규모 데이터 저장소에서 유용한 정보를 자동적으로 탐색하는 과정으로서, 데이터베이스를 구석구석 뒤져서 모른 채 넘어갈 수 있는 새롭고 유용한 패턴을 탐색하기 위해 고안된 방법이다[3]. 즉, 데이터에 숨겨진 패턴과 관계를 찾아내어 광맥을 찾아내듯이 정보를 발견해 내는 것을 뜻한다.

OLAP 과 데이터 마이닝은 기본적으로 데이터를 분석한다는 공통점을 가지고 있지만, 분석하는 데이터의 종류나 분석의 결과값은 서로 다르다. OLAP 에서 분석하는 데이터는 사실 데이터를 기반으로 하여 현재의 데이터의 현황이나 상태 등 표면값들을 보여 준다. 이에 반해, 데이터 마이닝은 다양하게 분포되어 있는 데이터들 사이에서 숨겨져 있는 지식값을 찾아낸다.

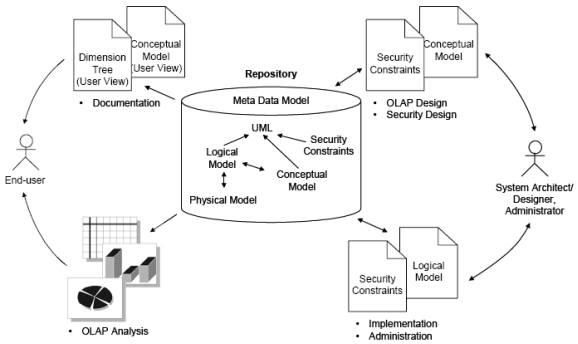
2.2. 기존 연구 비교 및 분석

[4]는 OLAP 환경 하에서 보안 방식 기법에 대한 연구 논문으로 데이터베이스의 기밀성, 무결성, 가용성의 고려를 강조하였다. 여기서 기밀성이란 허가되지 않은 검색이나 간접적인 추론에 의해 정보가 공개되어서는 안 되는 것을 말한다. 무결성은 올바른 제약 조건에 따라 제공되는 데이터가 정확한 상태를 유지해야 함을 말한다. 가용성은 사용자가 필요로 하는 데이터를 적시에 제공할 수 있어야 함을 말한다.

위와 같은 데이터 접근 제어를 위해 DAC(Discretionary access control), MAC(Mandatory access control) 등을 고려해 사용자에게 다양한 역할을 할당하는 방법을 세 가지 컨셉으로 설명하고 있다.

- SP(Simple predicate) – SP(S, A, O)
  역할, 접근타입, 보안객체를 사용
- SaP(Simple attribute predicate) – SaP(S, A, O, Attr)
  역할, 접근타입, 보안객체, 속성을 사용
- VBaP(Value based attribute predicate) – VBaP(S, A, O, Attr, value)
  역할, 접근타입, 보안객체, 속성, 속성값을 사용

MDX(Multidimensional Expressions)는 큐브 데이터를 위한 질의 언어로써 OLAP 에서 기본적으로 사용되는 연산을 지원한다. [4]에서는 OLAP 보안의 개념 및 논리 설계를 지원하기 위해 MDX 기반의 언어 MDSCL(multidimensional security constraint language) 를 제시하였다. 이는 기존 OLAP 보안의 개념적 모델링 방법[5]에서 제시한, 허가된 보안 객체로의 접근만을 허용하는(명시적 허가), 보안 정책을 OLAP 시스템의 개방성을 위해 명시적 거부의 정책으로 바꾸기 위함이다. 또한 복잡한 요구 사항을 충족시키기 위해 컬럼 단위의 비교 함수를 직관적으로 사용할 수 있도록 하였다.



(그림 1) MDSCL 및 UML 을 사용한 메타데이터 흐름 및 접근[6]

[6]에서 제시한 (그림 1)의 메타데이터를 통해 명시적 거부 정책을 사용한 접근 제어 방식은, OLAP 의 개방성을 향상시키는 데에는 성공하였지만, 권한 충돌 시 보안 정책에 대해서는 제시하지 않고 있다. 위와 같은 기존 연구를 바탕으로 본 논문에서는 보안성 강화를 위해 추가로 권한 충돌 시 최소한의 권한을 갖는 정책을 사용하였다.

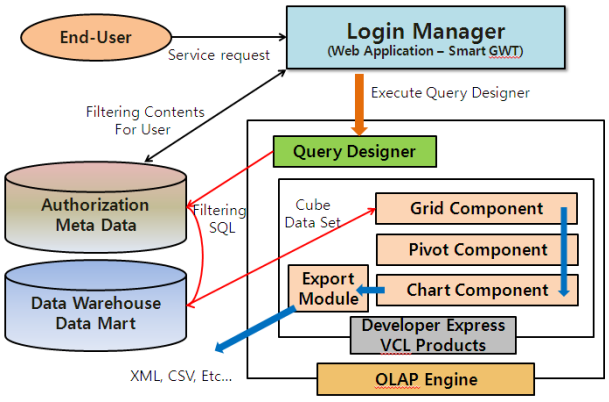
3. 설계 방안 및 구현

3.1. 설계 방안

본 논문에서는 [6]의 사용자 역할 할당에 대해 Authorization Meta Data Table 을 사용하여 관리한다.

이 시스템은 동적 문서를 생성하기 위하여 쿼리를 반영할 수 있는 표현 컴포넌트를 요구한다. OLAP 의 분석 결과는 관계형 데이터베이스에 대한 쿼리 결과셋을 연산하여 최종적으로 피벗 테이블의 형태를 갖는다. 본 논문에서는 데이터 접근 제어를 위한 SQL Generator 의 보안 모듈을 설계하고 OLAP 컴포넌트는 Developer Express VCL Products 를 사용한다.

OLAP 의 접근 대상 객체를 기능, 컨텐츠, 데이터로 분류하고, 프로그램 실행 시 각 객체에 대한 접근 권한을 DB 로부터 전달 받아 쿼리 편집기를 불러온다.



(그림 2) OLAP 시스템 구조

OLAP 시스템의 단계별 절차를 보면 다음과 같다.

먼저 최종 사용자는 Login Manager(사용자 인증, 권한 부여 모듈)에게 서비스를 요청한다. Login Manager는 Authorization Meta Data 로부터 접근이 허가된 컨텐츠 목록을 추출한다. 최종 사용자는 허가된 컨텐츠 매핑을 통해 Query Designer(질의 편집기 모듈) 서비스를 제공 받는다. 그 다음 작성된 사용자 질의(SQL)를 DW(Data warehouse), 또는 DM(Data Mart)에 요청을 하게 된다. 이 과정에서 Query Designer 내의 보안 모듈 GenerateSQLbeforeExecute 를 통해 최종 사용자에게 접근 허가 된 큐브 데이터 셋을 반환한다. 마지막으로 그 결과를 최종사용자에게 제공하여 Developer Express VCL Products 에서 제공하는 분석 업무를 수행한다.

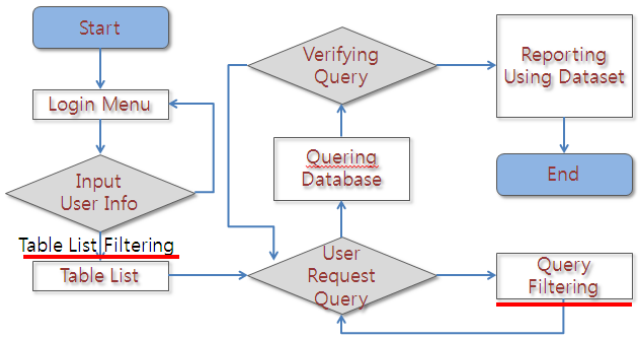
3.2. 구현

본 연구에서 구현한 OLAP 시스템은 OO 은행 정보계 시스템으로 운영되고 있으며, 데이터베이스의 사용자별 보안 정보를 사용하여, 데이터 접근 제어가 적용된 분석 업무를 지원하고 있다.

3.2.1. 구현 환경

플랫폼	x86, Intel Core i5
운영 체제	Windows 7
개발 언어	JAVA(SmartGWT), Delphi
서버	Apache Tomcat 7.0
데이터베이스	Sybase IQ 15.2

3.2.2. OLAP 작업 흐름도



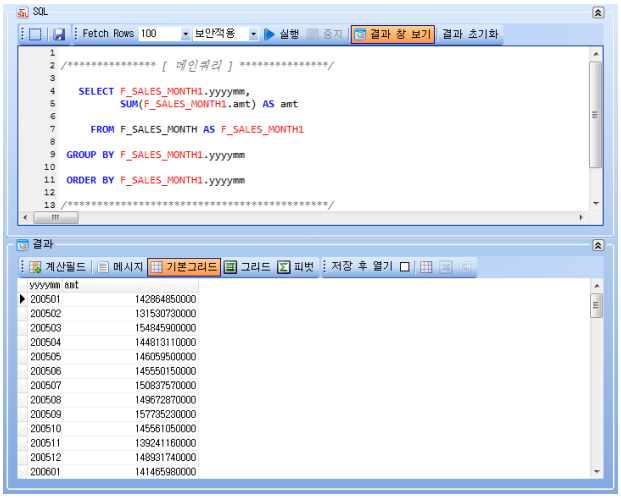
(그림 3) OLAP 흐름도

(그림 3)은 데이터 접근 제어 방법을 적용한 OLAP 시스템의 작업 흐름도를 나타낸다. 각 단계를 통해 사용자에게 할당된 권한과 접근 객체를 정의하고, 사용자 질의의 보안 필터링을 통해 허가되지 않는 데이터 접근을 방지한다. 이러한 일련의 과정들이 성능 저하를 가져올 수 있는 우려가 있지만, 실시간 OLAP 이 아닌 일반적인 OLAP 에서는 대용량의 분석 데이터를 가져오는 시간의 비중이 보안 모듈의 수행 시간에 비해서 월등히 크기 때문에 큰 문제가 되지는 않는다.

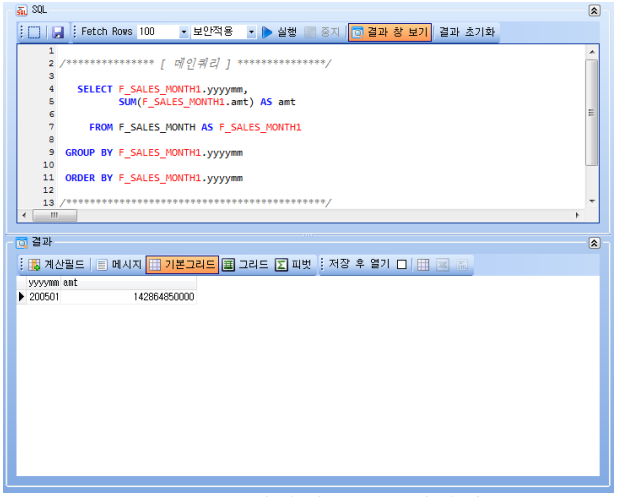
3.2.3. 결과 화면

다음 그림들은 본 논문에서 구현한 툴의 쿼리 실행 후의 화면이다. 각 화면의 SQL 문은 사용자가 Query Designer 를 통해 작성한 질의문이다. (그림 4)와 (그림 5)는 동일한 질의문을 사용하였지만, (그림 5)의 사용자는 [2005 년 1 월]의 데이터만을 조회할 수 있도록 보안이 적용되어 있다.

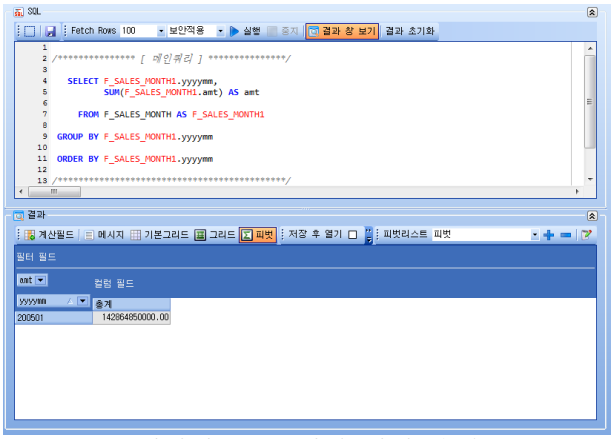
(그림 6)은 (그림 5)의 결과값을 이용하여 피벗 분석을 수행하는 화면이다.



(그림 4) 관리자 계정 질의



(그림 5) 데이터 접근 제어가 적용된 사용자의 질의



(그림 6) 데이터 접근 제어 질의 응답을 사용한 피벗 화면

4. 결론 및 향후 연구

다년간 쌓여 온 조직의 데이터 분석 수요를 충족시키기 위한 OLAP 툴은 최종 사용자의 폭이 전사로 확대되면서 IT 전문가를 통하지 않고도 대용량의 데이터를 손쉽게 분석할 수 있는 시대를 열었다. 또한 다양해진 최종 사용자 층에 따라 데이터 접근 제어에 대한 보안 이슈도 함께 증가했다. 이러한 OLAP 에 대한 연구는 대부분 XMLA, MDX 를 활용한 기능 중심적인 분석에 초점이 맞추어져 있고, 보안 이슈를 다루는 연구들은 컨셉 형식의 연구가 대부분이며 [2,4,5,6,7] MDX 에 종속적인 보안 적용 사례들이 주를 이룬다.

본 논문에서는 OLAP 의 보안 객체를 컨텐츠, 기능, 데이터로 보안 객체를 분류하고 MDX 쿼리를 보내기 전에 데이터 접근 제어 모듈을 사용하여 사용자별로 효율적인 큐브 데이터 셋을 얻을 수 있도록 구현하였다. 이렇게 만들어진 큐브 데이터 셋을 사용하여 최종 사용자는 허가된 데이터만을 가지고 데이터 분석 업무를 진행할 수 있다.

그러나 구현하고 다루었던 보안 객체는 데이터에 대한 데이터 접근 제어 방법이었기 때문에 향후 컨텐츠, 기능까지 확장된 OLAP 보안 객체에 대한 접근 제어와 권한 할당 제어를 구현하고자 한다.

참고문헌

[1] 천현진, 김동희, “인터넷&시큐리티 이슈(Vol 2010 No.11, 3 Net Trend)”, 한국인터넷진흥원, pp.35 (2010)

[2] Abello, A., Romero, O. “On-Line Analytical Processing”. In: Liu, L., • Ozsu, M.T. (eds.) Encyclopedia of Database Systems, pp. 1949-1954. Springer (2009)

[3] 용환승, 나연묵, 박종수, 승현우, 이민수, 이상준, 최린, “데이터 마이닝”. 인피니티 북스 (2007)

[4] Remzi kirgoze, Nevena Katic, Mladen Stolba, A Min Tjoa. “A Security Concept for OLAP”. IEEE Computer Society, (1997)

[5] Pernul, G., Winiwarter, W., Tjoa A M.: “The Entity-Relationship Model for Multilevel Security”. In Proc. 12th International Conference on the Entity-Relationship Approach (ER'93); Arlington, Texas, USA, December 15-17, (1993)

[6] PRIEBE T., PERNUL G., “A Pragmatic Approach to Conceptual Modeling of OLAP Security”, ER 2001: 20th International Conference on Conceptual Modeling, pp. 311-324, November 27-30, (2001)

[7] 최지웅, 김명호, “XMLA 를 사용한 OLAP 과 데이터 마이닝 분석이 가능한 리포팅 툴의 구현”, 정보과학회논문지 : 컴퓨팅의 실제 및 레터 제 15 권 제 3 호(2009.03)