http://dx.doi.org/10.3745/KIPSTC.2012.19C.2.091

OLAP 상에서 데이터 접근 제어 메커니즘 설계 및 구현

민 병 국[†] · 최 옥 경[††] · 김 강 석[†††] · 홍 만 표[††††] · 예 홍 진[†††††]

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. OLAP에서는 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 OLAP의 기능적인 분석에 치중하여 MDX(Multidimensional Expressions)와 XMLA(XML for Analysis) 등의 기법으로 기능을 구현하는 것에 그치고 있다. 이에 본 연구에서는 기존 연구의 문제점을 보완하기 위한 방법으로 효율적인 정보 보호를 위한 데이터 접근 제어 메커니즘을 제안하고 이를 설계 및 구현하였다. 제안한 데이터 접근 방법이 실제 OLAP 환경에서 효율성 있게 동작함을 확인하기 위해 실험평가를 수행하여 본 연구의 우수성을 입증하였다.

키워드 : OLAP, 데이터 접근 제어, 정보 보호

Design and Implementation of Data Access Control Mechanism based on OLAP

Byoungkuk Min[†] · Okkyung Choi[††] · Kangseok Kim[†††] · Manpyo Hong[††††] · Hongjin Yeh[†††††]

ABSTRACT

OLAP(On-Line Analytical Processing) is a tool to satisfy the requirements of managing overflowing data analysis. OLAP can provide an interactive analytical processing environment to every end-user. Security policy is necessary to secure sensitive data of organization according to users direct access database. But earlier studies only handled the subject in its functional aspects such as MDX(Multidimensional Expressions) and XMLA(XML for Analysis). This research work is purported for solving such problems by designing and implementing an efficient data access control mechanism for the information security on OLAP. Experimental evaluation result is proposed and its efficiency and accuracy are verified through it.

Keywords : OLAP, Data Access Control, Information Security

1. 서 론

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 IT전문가를 통해 조직의 데이터를 분석하고 보고서를 작성하여 조직의 의사 결정에 활용하였지만, 점점 늘어나는 데이터에 대한 분석 수요를 감당하기 어려워졌다.

OLAP은 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.

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

한국 IDC에 따르면 2010년 DBMS 시장은 11.6% 성장한 3,850억 원대 규모를 형성했다. 이는 비즈니스 인텔리전스(BI) 구현을 위해 DB 자원을 효율적으로 사용하기 위한 데이터웨어하우스, 데이터 통합, 비정형데이터를 포함한 데이

※ 본 연구는 지식경제부 및 한국인터넷진흥원의 "고용계약형 지식정보보안 석사과정 지원사업"의 연구결과로 수행되었음.
† 준 회 원 : 아주대학교 지식정보보안학과 석사
†† 정 회 원 : 아주대학교 지식정보보안학과 연구교수(공동교신저자)
††† 정 회 원 : 아주대학교 지식정보보안학과 연구교수
†††† 종신회원 : 아주대학교 정보통신전문대학원 교수
††††† 종신회원 : 아주대학교 정보컴퓨터공학부 부교수(교신저자)
논문접수 : 2011년 11월 18일
수 정 일 : 1차 2012년 2월 6일
심사완료 : 2012년 2월 29일

터의 관리/분석 수요가 확대되었기 때문으로 풀이되었다. 또한 2015년까지 매년 6.7% 의 성장을 전망했다[1]. 이렇게 성장하는 BI 시장과 함께 보안에 대한 이슈도 필수적으로 함께 다루어져야 한다.

본 연구에서는 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

2.1 OLAP

OLAP은 DW(Data Warehouse) 또는 특화된 DM(Data Mart)로부터 지식을 추출하여 의사 결정을 지원하는 시스템을 뜻한다. 주요 목적은 비전문가에게, IT 전문가의 개입 없이도, 다차원 데이터에 직접 접근하여 대화식으로 분석하고 Ad-Hoc 쿼리를 만들도록 하는 것이다[2].

OLAP은 큐브 데이터에 Slice, Dice, Drill-Down, Rollup 등의 기본 연산을 수행하여 최종적으로 피벗 분석을 통해 다차원 분석이 가능하도록 하고, 분석된 데이터를 통해 조직의 현황을 파악하고 의사 결정을 돕는 역할을 한다. 최근에는 예상 데이터를 이용한 시뮬레이션(Simulation), 플랜(Plan) 분석을 통해 앞으로 다가올 시장을 내다보기도 한다[3]. 또한 OLTP(On-Line Transactional Processing)와는 대조적으로 도입되어 서로 다른 요구 사항과 특징을 반영한다. 다음 <표 1>에서는 OLAP과 OLTP의 단적인 비교를 보여주고 있다[4].

〈표 1〉 OLAP과 OLTP의 비교

	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

2.2 기존 연구 비교 분석

OLAP은 다수의 사용자가 상호 작용하는 컴퓨팅 환경을 지니고 있고, 시스템에서는 민감한 정보를 효과적으로 보호하기 위해 다양한 접근 제어 정책들을 사용하고 있다. 이러한 접근 제어 정책은 정보의 소유자에 의하여 접근 통제 관계가 정의되는 임의적 접근 제어(Discretionary Access Control : DAC), 정보의 내용(보안등급)과 사용자나 그가 속한 그룹에 의하여 접근을 제어하는 강제적 접근 제어(Mandatory Access Control : MAC), 그리고 시스템 내에 필요한 역할(Role)과 그 역할이 수행할 수 있는 권한(연산)을 정의하고 각 사용자에게 역할을 할당하는 역할-기반 접근 제어(Role-Based Access Control : RBAC) 기법으로 나눌 수 있다[5][6].

본 연구에서는 이러한 접근 제어 정책들 중 DAC와 RBAC 정책을 기반으로 접근 권한 충돌 시 최소권한 유지에 대한 정책을 추가하여 보다 강화된 보안 정책을 제시한다.

[7]은 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, MAC 등을 고려해 사용자에게 다양한 역할을 할당하는 방법을 세 가지 컨셉으로 설명하고 있다.

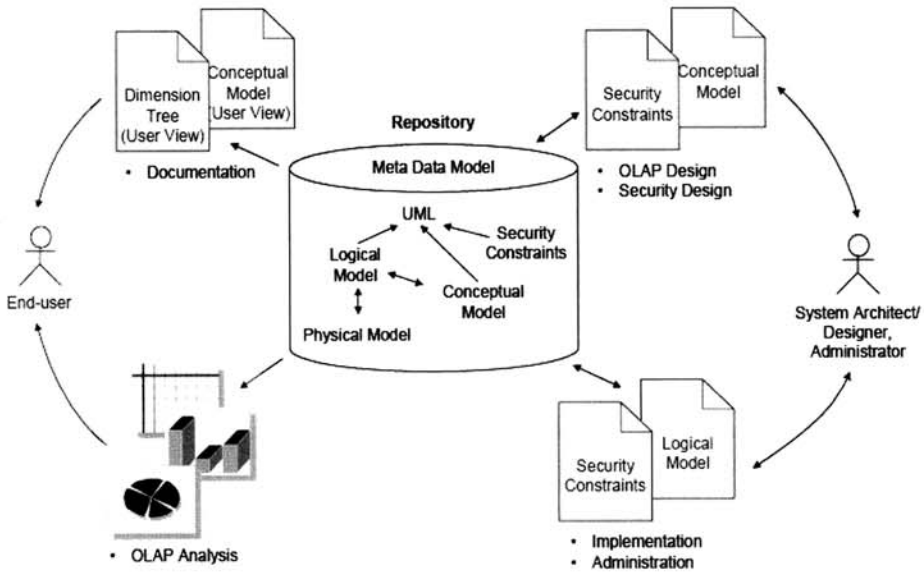
- SP(Simple predicate) : SP(S, A, O)
  역할, 접근타입, 보안객체를 사용
- SaP(Simple attribute predicate) : SaP(S, A, O, Attr)
  역할, 접근타입, 보안객체, 속성을 사용
- VBaP(Value based attribute predicate) :
  VBaP(S, A, O, Attr, value)
  역할, 접근타입, 보안객체, 속성, 속성값을 사용

본 연구에서는 위의 세 가지 컨셉들에 대한 설계와 구현을 위해 보안객체, 역할, 접근타입을 사용자UID를 중심으로 한 접근 제어 방식을 사용하였다. 이를 통해 기밀성, 무결성, 가용성을 확보할 수 있도록 하였다.

MDX(Multidimensional Expressions)는 큐브 데이터를 위한 질의 언어로써 OLAP에서 기본적으로 사용되는 연산을 지원한다. [8]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[9]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.

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

이는 현재 연구되고 있는 데이터 접근제어 방법과 큰 차이점을 가지고 있지는 않지만, [8]에서 제시한 메타데이터를



(그림 1) MDSCL을 사용한 메타데이터 흐름 및 접근

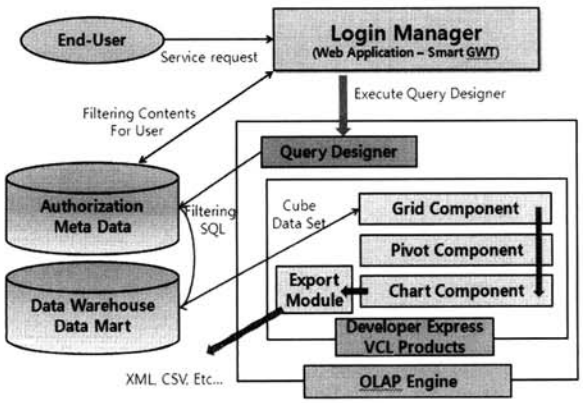
통한 명시적 거부 정책과 함께 최소 권한을 갖는 데이터 접근 제어 방식을 OLAP에 적용하여 보안 모듈이 얼마만큼 효율적으로 동작하는지에 그 목적을 두고 있다.

3. 설계 방안 및 구현

3.1 설계 방안

본 연구에서는 사용자 역할 관리를 위해 [8]의 사용자 역할 할당 구조 중 Authorization Meta Data Table을 사용하여 관리한다.

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



(그림 2) OLAP 시스템 구조

OLAP의 접근 대상 객체를 기능, 컨텐츠, 데이터로 분류하고, 프로그램 실행 시 각 객체에 대한 접근 권한을 DB로부터 전달 받아 쿼리 편집기를 불러온다.

OLAP 시스템의 단계별 절차를 보면 다음과 같다. 먼저 최종 사용자는 Login Manager(사용자 인증, 권한 부여 모듈)에게 서비스를 요청한다. Login Manager는 Authorization Meta Data로부터 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 GenerateSQLbeforeExecute를 통해 최종 사용자에게 접근 허가 된 큐브 데이터 셋을 반환한다. 마지막으로 그 결과를 최종사용자에게 제공하여 Developer Express VCL Products에서 제공하는 분석 업무를 수행한다.

3.2 보안 정책

OLAP은 최종 사용자로 하여금 직접 데이터베이스에 접근하여 자료를 분석할 수 있는 서비스를 제공하며, 또한 사용자나 그룹의 변화에 대해서도 빠르게 대응할 수 있는 관리 서비스를 제공한다. 이를 위해 관리되는 대상을 다음과 같이 3가지로 크게 나눌 수 있다.

첫 번째, 사용자 관리는 모든 접근 제어의 기본이 되는 관리 시스템이다. 이는 사용자에게 UID(Unique Identity)를 부여하여 그룹에 속하도록 하고 컨텐츠나 데이터 접근 시에 모든 접근 제어를 관리한다.

두 번째, 컨텐츠 관리는 OLAP에서 사용하는 모든 사용자 제공 객체라 할 수 있다. 컨텐츠에는 분석 결과 테이블, 분석 결과 테이블을 이용하여 다차원 분석을 수행하는 피벗 테이블, 분석 된 결과를 그래프로 나타내는 차트, 여러 가지

분석 결과 화면들을 모아 한 곳에서 보여주는 대시보드, 사용자가 필요에 따라 저장하고 불러올 수 있는 모든 파일들이 속할 수 있다. 이러한 컨텐츠는 공유 폴더와 개인 폴더를 통해 다른 사용자와 커뮤니케이션에 이용하거나 본인만의 분석 보고서를 만들고 사용하는 서비스를 제공하는 기본이 된다.

세 번째, 데이터 관리는 사용자가 작성한 쿼리에 대한 검증 및 변환을 수행한다. 각 사용자에게 접근이 허용된 테이블을 검사하며 그에 맞지 않는 테이블에 대한 요청은 기각한다. 또한, 접근 가능한 테이블 내에서도 사용자에게 보여주면 안되는 정보에 대해서 Filtering SQL 을 수행하여 각 보안 정책에 따른 쿼리만을 수행하도록 도와주는 역할을 한다.

또한 보안 대상에 대한 권한도 크게 두 가지로 나누어 관리한다. OLAP에서 사용되는 관리자 모드 접근, 컨텐츠 접근, 테이블 접근 등 서비스 접근 제어와 관련된 접근 권한이 있는 반면, 서비스에 접근할 때 수행할 수 있는 기능들에 대한 권한이 있다.

기본 값은 프로그램 초기 값이나 관리자가 정해 놓은 값을 의미한다. OLAP 시스템에서는 기본 접근 컨텐츠인 공유 폴더와 개인폴더에 대한 접근, 분석의 기본 기능인 데이터 모델 작성, 쿼리 작성 및 피벗 테이블 작성이 된다.

사용자가 가지는 그룹이 삭제되어도 다른 그룹에 속해서 상속이 여전히 유효한 경우가 있다. 이 경우는 삭제 된 그룹에서만 가지던 최소 권한을 해제하고 현재 속해 있는 그룹들의 권한과 사용자에게만 특별히 부여된 스페셜 권한이 모두 유효하게 된다.

사용자의 그룹이 변경 된 경우에는 조금 복잡한 프로세스를 가지게 된다. 새롭게 소속되는 그룹이 가지는 권한 중에 최소 권한이 있는지 검사하여 해당 최소 권한을 부여하고, 기존에 속했던 그룹만이 가지는 최소 권한이 있는지 검사한 후 기존 그룹의 최소 권한을 해제한다.

이렇게 함으로 사용자와 그룹에 대한 추가/삭제/변경 시 권한의 상속과 부여, 해제에 관해 정의하였다.

위와 같은 권한 부여 정책을 사용한 그룹과 사용자의 변경에 따른 권한 검사는 구현 코드에 있어서 조금은 복잡한 프로세스를 가지게 된다. 여러 테이블을 참조하여 얻어 온 결과를 다시 새롭게 부여할 그룹에 대한 결과와 비교하여 권한을 부여하는 과정이 추가되기 때문이다. 하지만 이렇게 권한을 부여할 때에 수행하는 검사와 권한 부여 과정을 통해 사용자 UID로 통합된 메타데이터 환경에서 더욱 빠른 성능과 간편한 관리자 모드를 지원할 수 있다.

본 연구에서 구현하는 보안이 적용된 OLAP에서는 [8]에서 설명하는 DAC와 RBAC의 기본 개념을 구현하고, 추가로 최소 권한에 대한 보안 정책을 가지고 있다.

위에서 설명한 권한 부여는 사용자와 그룹에 대해 모두 적용이 가능하다. 그렇기 때문에 사용자와 그룹, 그룹과 그룹 간의 서로 다른 권한이 사용자에게 부여될 수 있다. 이러한 권한 충돌 시에 다음과 같은 정책을 적용하여 권한 충돌 시 최소 권한을 가짐으로 보안을 강화하도록 한다.

예시) 그룹1 - 사용자1, 사용자2
그룹2 - 사용자2

〈표 2〉 권한 충돌 시 최소 권한 부여 정책

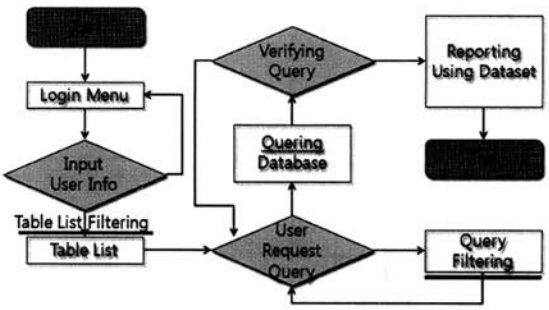
권한 충돌 예시	
기능 권한 충돌 (대시보드 기능) 그룹1 - 허용 그룹2 - 거부	사용자1 - 대시보드 사용 가능 사용자2 - 대시보드 사용 불가능
디렉토리 권한 충돌 ([폴더1]에 대한 권한) 그룹1 - 읽기/쓰기 그룹2 - 읽기	사용자1 - 읽기/쓰기 가능 사용자2 - 읽기 가능
데이터 접근 권한 충돌 ([테이블1]에 대한 접근) 그룹1 - 허용 그룹2 - 거부	사용자1 - 테이블1 접근 가능 사용자2 - 테이블1 접근 불가능
컨텐츠 접근 권한 충돌 (읽기 권한이 있는 [보고서a]에서 [테이블1을 사용할 경우)	사용자1 - 보고서a 사용 가능 사용자2 - 보고서a 실행 시 수행거부 에러메시지 발생(권한 없는 테이블 접근)

3.3 구현

본 연구에서 구현한 OLAP 시스템은 조직의 정보계 시스템으로 운영될 수 있으며, 데이터베이스의 사용자별 보안 정보를 사용하여, 데이터 접근 제어가 적용된 분석 업무를 지원할 수 있다.

〈표 3〉 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(DW), PostgreSQL (Meta Data)

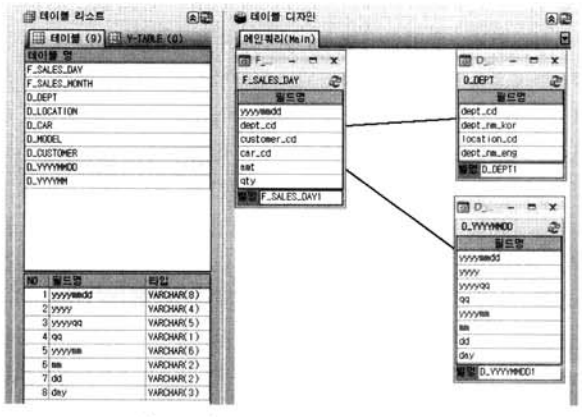


(그림 3) OLAP 흐름도

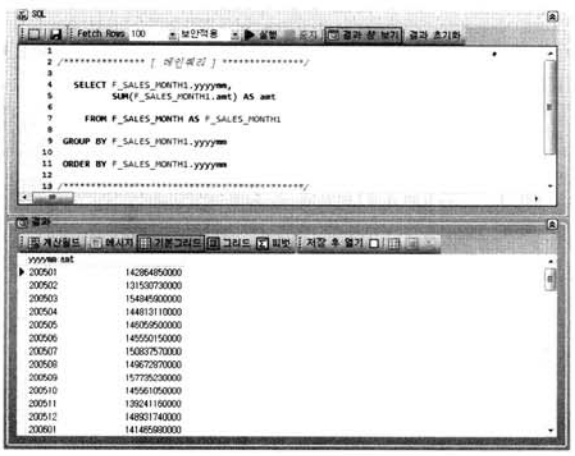
(그림 3)은 데이터 접근 제어 방법을 적용한 OLAP 시스템의 작업 흐름도를 나타낸다. 사용자의 로그인 시점에서 사용자에게 접근 가능한 데이터를 담고 있는 테이블과 컬럼 정보가 정해지게 된다. 사용자는 제공된 테이블과 컬럼 정보를

이용하여 Ad-Hoc 쿼리를 생성할 수 있다. 생성된 쿼리를 통해 DBMS에 데이터를 요청하면 쿼리 필터링 모듈은 사용자의 쿼리를 분석하여 접근 가능한 데이터만을 필터링하게 된다. 필터링된 쿼리의 구문 검사가 완료되고 성공적으로 쿼리가 생성되면 DBMS는 필터링된 결과를 사용자에게, 사용자가 어떠한 데이터에 대해서 필터링 되었는지에 대한 사실을 알 필요 없이, 접근 권한에 알맞은 정보를 제공하게 된다. 마지막으로 사용자는 제공된 정보를 필터링, 피벗, 차트, 대시보드 등 사용하기 쉬운 형태로 분석하여 의사결정에 활용하도록 한다. 각 단계는 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 OLAP이 아닌 일반적인 OLAP 에서는 대용량의 분석 데이터를 가져오는 시간의 비중이 보안 모듈의 수행 시간에 비해서 월등히 크기 때문에 큰 문제가 되지는 않는다[10].

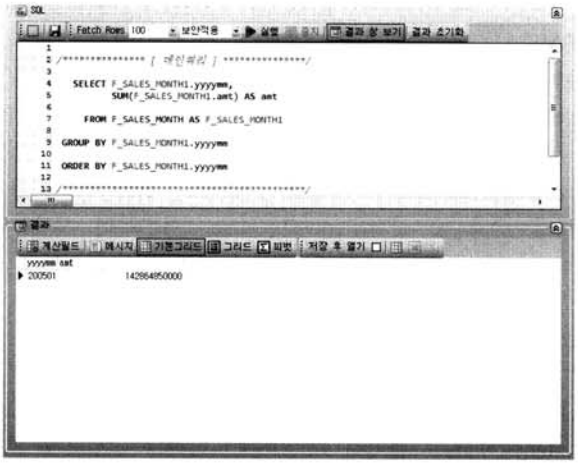
다음 그림들은 본 연구에서 구현한 툴의 쿼리 실행 후의 화면이다. 각 화면의 SQL문은 사용자가 Query Designer를 통해 작성한 질의문이다. 사용자는 최초 접근이 허가 된 테이블의 컬럼들을 사용하여 데이터 모델을 생성한다. 마우스 드래그와 클릭을 통해 여러 가지 집계 결과를 가질 수 있는 Fact 테이블과 Dimensional 테이블을 연결한다.



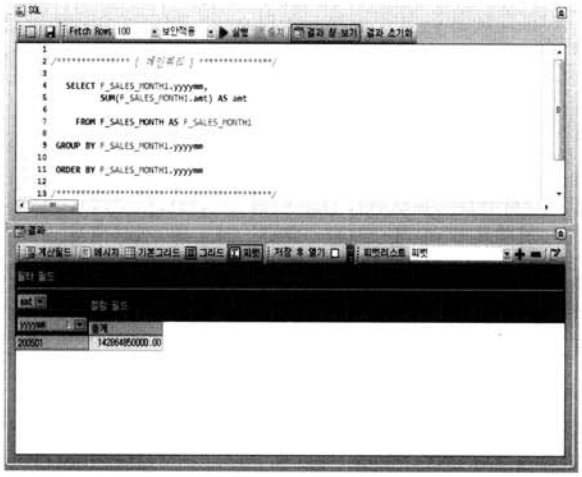
(그림 4) 데이터 모델 작성 화면



(그림 5) 관리자 계정 질의



(그림 6) 데이터 접근 제어가 적용된 사용자의 질의



(그림 7) 데이터 접근 제어를 사용한 피벗 화면

(그림 5)와 (그림 6)은 (그림 4)에서 작성된 데이터모델을 기초로 Ad-Hoc 쿼리를 수행한 후 그 결과 값을 보여주고 있다. (그림 5)와 (그림 6)은 동일한 질의문을 사용하였지만, (그림 6)의 사용자는 [2005년 1월]의 데이터만을 조회할 수 있도록 보안이 적용되어 있다.

(그림 7)은 (그림 6)의 결과값을 이용하여 피벗 분석을 수행하는 화면이다.

4. 실험 평가

4장에서는 본 연구에서 구현한 OLAP 보안 모듈의 성능 평가를 수행한다. OLTP와 다르게 분석 요구 사항이 발생할 경우 한시적으로 접근하여 데이터 분석을 처리하는 OLAP의 특성상 중요한 테스트 항목은 보안 모듈의 수행 시간이 전체 쿼리 수행 시간에 미치는 영향으로 정의한다.

4.1 실험 환경

실험의 결과는 시스템의 사양과 운영체제, 데이터베이스의 종류, 테이블의 구조, 데이터의 종류에 따라 다를 수 있다.

구현된 OLAP 시스템에서의 컨텐츠는 PostgreSQL DBMS에 데이터를 요청하고 받아온 데이터를 json (JavaScript Object Notation)의 형태로 parsing 하여 제공하도록 되어 있다. 사용자가 실제로 서비스를 받기까지 걸리는 시간은 로그인을 수행한 사용자의 UID를 사용하여 접근 가능한 컨텐츠 목록을 받기 위해 Client는 Server에 사용자 UID를 넘겨 준 시간(Request Time : Rt)부터 시작된다. Server는 받은 사용자UID를 통해 PostgreSQL에 컨텐츠 목록을 요청하는 쿼리(Execute Query Time : Eqt)를 보낸다. Server는 쿼리의 결과를 json의 형태로 parsing 하여 Client에 제공(Parsing Json Time : Pjt)한다. Client는 받은 컨텐츠 json 정보를 사용하여 사용자에게 서비스를 제공(Display Contents Time : Dct)한다. 이후 Client에서 컨텐츠에 대한 접근 시에는 초기에 제공받은 컨텐츠 정보를 가지고 있기 때문에 별도의 Fetch 작업을 수행하지 않고도 사용자에게 허가된 컨텐츠에 접근할 수 있다.

$$\text{Total Access Time} = Rt + Eqt + Pjt + Dct$$

위의 시간에서 가장 크게 시간에 영향을 미치는 부분은 Pjt와 Dct이다. 또한 Eqt와 Dct의 시간이 변경되는 요인으로는 컨텐츠의 수가 된다. 그렇기 때문에 실험에서는 변수로 컨텐츠의 수를 사용한다. 컨텐츠의 수가 100개, 1000개 10000개, 100000개 일 때의 서비스 제공 시간을 측정하여 OLAP 서비스에서의 접근 제어 성능을 평가하고자 한다.

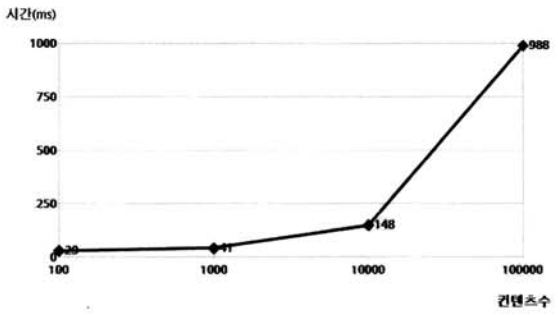
또한, 사용자가 작성한 Ad-Hoc 쿼리가 DBMS로 전달되기 전에 적용되는 보안 필터링 모듈의 수행 시간을 측정하여 전체적인 쿼리 수행 시간에 미치는 영향을 평가하도록 한다.

보안 필터링에 소요되는 시간은 구문 검사 시간, 사용자 데이터 필터링 정보 요청/응답 시간, 쿼리 리빌딩 시간이 포함된다. 필터링 되는 데이터에 따라 리빌딩 된 쿼리문이 지연시키는 시간을 측정하도록 한다.

실험에 사용되는 데이터셋은 OLAP에서 일반적으로 사용하는 Star-Schema의 형태로 구성하도록 한다. 각 쿼리문에서 필터링이 수행되는 구간을 Fact 영역과 Dimension 영역으로 나누어 여러 가지 조건별 쿼리 수행 시간을 측정하도록 한다.

4.2 실험 결과

사용자가 로그인을 한 후 본인에게 해당되는 컨텐츠의 수에 따른 속도를 측정한 결과 10만건 이하 일 때는 1초 이내의 속도가 측정되었다. 보통 OLAP 시장에서 하루에 적으면 1건에서 많으면 25건 정도의 화면을 개발할 수 있다. 물론 만드는 사람이 많아지면 더 많이 만들 수도 있다. OLAP 프로젝트의 특성에 따라 다르지만 일반적으로 기업에서 사용하는 화면은 10,000개가 넘는 경우도 거의 드물고, 결과 값은 컨텐츠 수가 10,000건 이하일 경우 대략 0.15초 내에 사용자가 접근할 수 있는 컨텐츠를 제공해 줄 수 있는 성능을 보여주고 있다.



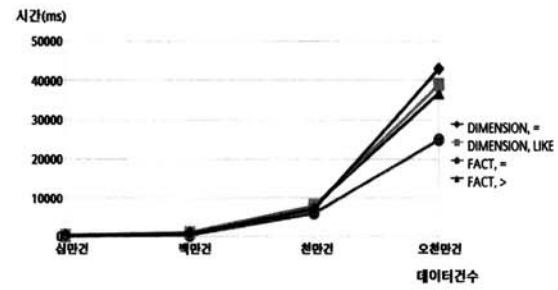
(그림 8) 컨텐츠 수에 따른 서비스 응답 시간

측정 시간 중 DBMS의 컨텐츠 목록 응답 쿼리 수행 시간은 약 40% 정도를 차지한다. 나머지 50% 정도는 클라이언트에서 화면 처리에 쓰이는 시간이다. 즉, 동시 접속자가 발생할 시 DBMS 서버에 걸리는 부하는 1초 내에 응답할 수 있는 응답자의 수를 이론적으로 500명으로 볼 수 있다.

사용자가 작성한 쿼리문이 보안 필터링 모듈을 거치며 본래의 요청한 데이터보다 더 작은 데이터를 검색하고 반환하도록 수행되었다. 이는 인덱스, 클러스터링 여부 등에 따라 차등이 생기지만 대체적으로 본래의 쿼리 수행 속도보다 더 빠른 결과를 보여주었다. 또한 사용자별 조건을 검색하는 보안 모듈의 경우 10ms 이내의 시간이 소요되었고, 전체적인 쿼리가 수행되는 시간에 비례해서, 아주 작은 수행 속도라고 볼 수 있다.

데이터건별, 컬럼타입별, 조건연산자별 수행 시간에 대한 결과를 (그림 9)로 표현하였다. 데이터건별에 따라 수행 시간이 증가는 것은 데이터베이스의 처리속도가 그만큼 오래 걸리는 것을 반영한다. 데이터건수 10만건에서 5천만건 사이의 쿼리 수행속도를 측정한 결과 0.1초 이내에서 수 십초 내지 수 분까지 소요되는 것을 확인할 수 있다. 보안 모듈에서 사용되는 10ms의 시간은 데이터 건수에 관계없이 일정하다. 컬럼 타입별 쿼리 수행 시간을 측정한 결과는 수치를 검색하는 FACT와 문자열을 검색하는 DIMENSION을 기준으로 측정하였다. 그 결과 문자열보다 상대적으로 컴퓨터의 비교 속도가 빠른 수치 값을 통한 필터링 결과가 조금 더 빠른 쿼리 수행 시간을 사용하고 있음을 보여주고 있다.

(그림 9)에서 보여주는 조건 연산자별 쿼리 수행 시간에서는 결과적으로 FACT(=) > FACT(>) > DIMENSION (LIKE) > DIMENSION(=) 의 순서대로 측정되었다.



(그림 9) 쿼리 수행 시간(단위 : ms)

일반적으로 "LIKE" 비교보다 "=" 비교가 더 빠른 비교 속도를 보여주지만 현재 테스트에서 사용한 샘플 데이터는 CHAR가 아닌 VARCHAR를 사용하기 때문에 조금은 상이한 결과가 나타났다. 실제 OLAP을 사용하는 많은 기업들이 CHAR와 VARCHAR를 혼재해서 사용하기 때문에 데이터타입에 따라 실험 결과는 다르게 나타날 수 있다. [그림 9]의 결과는 VARCHAR를 사용할 때 "="와 "LIKE" 검색을 사용 목적에 따라 어떻게 사용하면 좋을지 참고하는 자료가 될 수 있다.

5. 결 론

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 OLAP에 대한 연구는 대부분 XMLA, MDX를 활용한 기능 중심적인 분석에 초점이 맞추어져 있고, 보안 이슈를 다루는 연구들은 컨셉 형식의 연구가 대부분이며[4, 7, 8, 9, 11] MDX에 종속적인 보안 적용 사례들이 주를 이룬다.

본 연구에서는 OLAP의 보안 객체를 컨텐츠, 기능, 데이터로 보안 객체를 분류하고, 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 사용하여 데이터 분석 업무를 진행할 수 있다. 이를 통해 기존 연구에서 다루지 않았던 OLAP 보안 적용에 대한 연구와 기밀성, 무결성, 가용성을 보장하는 보안 모듈에 대한 설계 및 구현을 연구하였다.

구현된 보안 모듈들은 보안 객체에 대한 분류를 정의하고, 접근 제어를 수행하고, 최종적으로 사용자의 쿼리를 분석하여 권한에 속해 있는 데이터셋만을 반환하도록 설계되었다. 이 과정에서 보안 모듈의 수행 시간은 컨텐츠 수에 따라 1초 이내에서 증가하는 결과를 보여주었지만, 이는 컨텐츠수가 1만건일 때를 가정했을 경우이기 때문에 이보다 훨씬 작은 시간만이 소요될 수 있다. 또한 쿼리 필터링 보안 모듈의 시간은 데이터에 상관없이 메타데이터에서 사용자의 데이터 접근 조건을 검색하는 시간인 10ms 이내의 시간만을 사용함으로 전체적인 쿼리 수행 시간에 큰 영향을 미치지 않았고, 필터링 된 쿼리를 통해 더 작은 데이터셋을 반환함으로 전체 쿼리 수행 시간을 줄이는 효과를 보여주고 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. 또한, 쿼리에 따라 불규칙적인 성능 평가 결과를 보여주었던 부분에 대해서 보안 필터링 모듈에 대한 알고리즘에 대한 추가적인 연구가 필요할 것이다.

참 고 문 헌

[1] 한국IDC, "한국 DBMS(Database Management System) 시장 분석 및 전망 보고서, 2011-2015>", 2011.

[2] Erik Thomasen, "OLAP Solutions : Building Multidimensional Information Systems", John Wiley & Sons, ISBN: 0471400300, 2002.

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

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

[5] S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models", IEEE Computer, Vol.29, No.2, pp.38-47, 1996.

[6] X. Zhang, J. Park, and R. Sandhu, "Schema based XML Security: RBAC Approach," IFIPWG 11.3, pp.300-343, 2003.

[7] Remzi kirgoze, Nevena Katic, Mladen Stolba, A Min Tjoa. "A Security Concept for OLAP". IEEE Computer Society, 1997.

[8] 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.

[9] 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.

[10] Lingyu Wang and Sushil Jajodia, "Security in Data Warehouses and OLAP Systems", in Handbook of Database Security: Applications and Trends, Michael Gertz and Sushil Jajodia, editors, Springer, New York, 2008.

[11] 최지웅, 김명호, "XMLA를 사용한 OLAP과 데이터 마이닝 분석이 가능한 리포팅 툴의 구현", 정보과학회논문지 : 컴퓨팅의 실제 및 레터 제 15권 제 3호, 2009, 03.

민 병 국

e-mail : bkmin@ajou.ac.kr

2012년 아주대학교 지식정보보안학과 (공학석사)

2012년~현 재 (주)엠투소프트 기술연구소 연구원

관심분야 : OLAP, Data Warehouse, MIS, Access Control Security, Financial Security

최 옥 경

e-mail : okchoi@ajou.ac.kr
2006년 중앙대학교 컴퓨터공학부 (공학박사)
2011년~현 재 아주대학교 지식정보보안학과 연구교수
관심분야 : Semantic Web Services System, e-Commerce, Auction, Information Retrieval,, Mobile Cloud Computing Security, Mobile/Wireless Network Security

김 강 석

e-mail : kangskim@ajou.ac.kr
2007년 인디애나 컴퓨터공학과(공학박사)
2010년~현 재 아주대학교 지식정보보안학과 연구교수
관심분야 : mobile computing, ubiquitous computing, scalable distributed database system, floor control, mobile applications with smart phones, mobile security, data mining and bioinformatics

홍 만 표

e-mail : mphong@ajou.ac.kr
1991년 서울대학교 전산학과(이학박사)
2011년~현 재 아주대학교 정보통신전문대학원 교수
관심분야 : Mobile Security, Ubiquitous System

예 홍 진

e-mail : hjyeh@ajou.ac.kr
1993년 Universite Joseph Fourier-Ecole Normale Superieure de Lyon (France), 공학박사(전자계산학)
1993년~현 재 아주대학교 정보컴퓨터공학부 부교수
관심분야 : Information Security, Mobile Security, Application Security