다양한 크기의 데이터 그룹에 대한 접근 제어를 지원하는 데이터베이스 보안 시스템

정 민 아[†] · 김 정 자[††] · 원 용 관[†††] · 배 석 찬[††††]

요 약

최근 병원 및 은행 등의 대규모 데이터베이스에 접근하는 사용자의 요구 사항이 다양해짐에 따라 데이터베이스 보안에 대한 중요성도 커졌다. 기존의 접근 제어 정책을 이용한 데이터베이스 보안 모델들이 존재하지만 이들은 복잡하고, 다양한 유형의 접근제어를 원하는 사용자의 보안 요구를 충족시키지 못한다. 본 논문에서는 데이터베이스를 접근하는 각 사용자별로 다양한 크기의 데이터 그룹에 대한 접근 제어를 제공하며, 임의의 정보에 대한 사용자의 접근 권한의 변화를 유연하게 수용하는 데이터베이스 보안 시스템을 제안하였다. 이를 위해 다양한 크기의 데이터 그룹을 테이블, 속성, 레코드 키에 의해 정의하였고, 사용자의 접근 권한은 보안 등급, 역할과 보안 정책들에 의해 정의하였다. 제안하는 시스템은 두 단계로 수행된다. 제 1단계는 수정된 강제적 접근 제어(Mandatory Access Control : MAC)정책과 역할 기반 접근 제어(Role-Based Access Control : RBAC)정책에 의해 수행된다. 이 단계에서는 사용자 및 데이터의 보안 등급과 역할에 의해 접근이 제어되며, 모든 형태의 접근 모드에 대한 제어가 이루어진다. 제 2단계에서는 수정된 임의적 접근 제어(Discretionary Access Control : DAC)정책에 의해 수행되며, 1단계 수행결과가 다양한 크기의 데이터 항목에 대한 read 모드 접근제어 정책에 따라 필터링되어 사용자에게 제공한다. 이를 위해 사용자 그룹은 보안 등급에 의한 그룹, 역할에 의한 그룹, 사용자 부분집합으로 이루어진 특정 사용자 그룹으로 정의하였고 ***Block(s, d, r)*** 정책을 정의하여 특정 사용자 s가 특정 데이터 그룹 d에 'read' 모드, r로 접근할 수 없도록 하였다. 제안한 시스템은 사용자별 데이터에 대한 접근 제어가 복잡하게 요구되는 특정 유전체 연구 센터의 정보에 대한 보안 관리를 위해 사용하였다.

A Database Security System supporting Access Control for Various Sizes of Data Groups

Mina Jeong[†] · Jungja Kim[††] · Yonggwan Won[†††] · Sukchan Bae[††††]

ABSTRACT

Due to various requirements for the user access control to large databases in the hospitals and the banks, database security has been emphasized. There are many security models for database systems using wide variety of policy-based access control methods. However, they are not functionally enough to meet the requirements for the complicated and various types of access control. In this paper, we propose a database security system that can individually control user access to data groups of various sizes and is suitable for the situation where the user's access privilege to arbitrary data is changed frequently. Data group(s) in different sizes d is defined by the table name(s), attribute(s) and/or record key(s), and the access privilege is defined by security levels, roles and polices. The proposed system operates in two phases. The first phase is composed of a modified MAC (Mandatory Access Control) model and RBAC (Role-Based Access Control) model. A user can access any data that has lower or equal security levels, and that is accessible by the roles to which the user is assigned. All types of access mode are controlled in this phase. In the second phase, a modified DAC(Discretionary Access Control) model is applied to re-control the '*read*' mode by filtering out the non-accessible data from the result obtained at the first phase. For this purpose, we also defined the user group s that can be characterized by security levels, roles or any partition of users. The policies represented in the form of ***Block(s, d, r)*** were also defined and used to control access to any data or data group(s) that is not permitted in '*read*' mode. With this proposed security system, more complicated '*read*' access to various data sizes for individual users can be flexibly controlled, while other access mode can be controlled as usual. An implementation example for a database system that manages specimen and clinical information is presented.

키워드 : 데이터베이스 보안(Database Security), 접근 제어(Access Control), 시료 및 임상 정보 관리(Specimen and Clinical Information Management)

1. 서 론

은행, 대학, 병원, 도서관, 중앙 행정 및 지방 행정 기관 등의 공공 및 사설 단체에서 사용되는 데이터베이스 규모가 커지고, 이러한 데이터베이스에 대한 사용자의 접근 요구사항이 다양해짐에 따라 데이터베이스 보안에 대한 중요성도 커졌다. 최근 대부분의 관계형 데이터베이스 관리 시스템은 몇 가지 제한된 보안 기법들만을 제공하고 있는데, 이러한 데이터베이스 보안 기법들은 주로 정책기반 접근 제어(policy-based access control)를 이용하고 있다[1].

기존에 사용되고 있는 대표적인 접근제어 정책으로는 강제적 접근 제어(Mandatory Access Control : MAC), 임의적 접근 제어(Discretionary Access Control : DAC), 역할 기반 접근 제어(Role-Based Access Control : RBAC)등이 있다.

† 정 회 원 : 전남대학교 전자통신기술연구소 Post-Doc.
†† 준 회 원 : 전남대학교 전자통신기술연구소 Post-Doc.
††† 종신회원 : 전남대학교 컴퓨터공학과 교수
†††† 종신회원 : 군산대학교 컴퓨터정보과학과 교수
논문접수 : 2003년 4월 8일, 심사완료 : 2003년 10월 2일

MAC 정책은 데이터와 사용자에 대하여 보안 등급을 부여하고 이를 통하여 정보의 비정상적인 흐름을 제어할 수 있다. 이는 복잡한 접근 제어를 위한 조건을 만족할 수 있는 유동성이 부족하다는 단점이 있다[2]. DAC 정책은 MAC 정책에 비하여 보다 유동적인 접근 제어가 가능한 반면, 인증된 사용자로부터 인증되지 않은 사용자로의 정보 흐름을 제어할 수 없는 단점이 있다[3]. RBAC 정책은 사용자가 적절한 역할에 할당되고 각 역할에 할당된 접근권한에 따라 정보에 접근할 수 있다. 그러므로 RBAC 정책은 보안관리를 단순하게 할 수 있으며, 사용자에게 최소한의 권한만을 허용하여 권한의 남용을 방지할 수 있다[4, 5].

이러한 각 접근 제어 정책의 특성 등을 고려하여 데이터베이스 시스템을 위한 보안 모델들이 제안되어 왔다. 강제적 접근 제어 정책을 이용한 모델로는 Access Matrix 모델, Task-Grant 모델, Action-Entity 모델, Wood등이 제안한 모델등이 있으며, 임의적 접근 제어 정책을 이용한 모델로는 Jajodia-sandhu 모델과 Smith-Winslett 모델이 있다[6-9]. 또한, 강제적 접근 제어 정책과 임의적 접근 제어 정책을 조합하여 제안한 모델로는 Sew View 모델이 있다[10]. 단순한 보안 관리를 제공하는 역할 기반 접근 제어 정책에 관해서는 Sandhu-Bhamidipati와 Ferraiolo등에 의하여 연구가 이루어지고 있다[11, 12].

이러한 모델들에서 정의한 보안 정책들은 보안 분류 등급을 고려하기 위해 표준 관계형 모델을 확장하였다. 그러나 사용자의 보안 요구 사항이 수시로 변할 경우 변경이 용이하지 않는 단점이 있다. 즉, 임의의 데이터에 대한 사용자의 접근 권한이 수시로 변동되는 상황에 융통성있게 대처하고, 공통된 하나의 정보에 대하여 각 사용자 별 접근 제어를 제공하지 못한다. 예를 들어, 유전체 연구정보센터(genome research information center)에서 시료 및 임상 데이터베이스(specimen and clinical database)에 접근하는 임의의 두 사용자가 특정 테이블의 동일한 속성에 대한 접근은 가능하지만, 그 속성의 각 튜플들에 대한 접근은 상이할 경우 기존의 보안 모델로는 접근 제어가 용이하지 않는 경우가 발생한다. 이는 속성보다 작은 크기의 데이터 항목에 대한 접근 제어가 용이하지 않음을 의미한다. 또한, 특정 환자 데이터에 대한 접근 권한을 가진 사용자가 그 데이터에 대한 접근 권한을 갖지 않은 사용자에게 그 데이터 중 일부 데이터에 대한 접근 권한을 부여하는 상황이 요구되기도 한다. 예를 들어, 센터의 총 책임자는 검체골수 테이블에 접근하는 권한을 갖고 있으며, 연구원은 같은 테이블에 접근하는 권한을 갖고 있지 않을 경우, 총 책임자가 검체골수 테이블의 특정 데이터 항목에 대한 접근 권한을 연구원에게 부여해야 하는 상황이 발생할 수 있다. 따라서, 이와 같은 문제점을 해결하기 위해서는 다양한 튜플과 속성의 조합으로 구성되는 서로 다른 크기의 데이터 그룹에 대한 세부적인 접근 제어가 필요하다.

본 논문에서는 서로 다른 크기의 데이터 그룹에 대한 세부적 접근 제어를 위한 시스템을 제안한다. 제안한 시스템은 데이터와 사용자가 등급화된 환경에서 강력한 보호가 필요한 대량 정보에 주로 적용되는 강제적 접근 제어를 기반으로 다른 정책 기반 접근제어들을 조합 및 변형하였다. 또한 데이터 입력에 따른 보안 등급 부여는 사용자의 보안등급을 따를 경우 정책의 혼란을 야기할 수 있어 데이터 관리자가 부여하도록 하였다. 제 1단계에서 수정된 강제적 접근 제어 및 역할 기반 접근 제어 정책을 조합하고, 제 2단계에서는 세부적 접근 제어를 위하여 임의적 접근 제어를 변형하여 적용하였다. 이를 위해 먼저, 사용자 그룹 및 데이터 그룹을 정의하고, 이를 기반으로 보안 정책을 설정하였다. 본 논문에서 제안한 시스템은 데이터베이스의 보안을 위해 표준 관계형 모델을 확장하지 않고, 사용자별로 상이한 접근 규칙을 제공함으로써 복잡한 제어 구조를 다룰 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 접근 제어 정책 및 데이터베이스 보안 모델들에 관한 관련 연구를 기술하고 3장에서는 본 논문에서 제안하는 접근 제어를 위한 사용자 및 데이터에 관하여 정의한다. 4장에서는 접근 제어를 위한 보안 요구사항을 기술하고, 5장에서는 제안한 시스템의 구조, 각 모듈별 기능 및 구현 결과를 기술한다. 마지막으로 6장에서는 결론을 맺는다.

2. 접근 제어 정책 및 데이터 베이스 보안 모델

2.1 MAC Policy

강제적 접근 제어 정책은 Bell과 LaPadula가 운영체제를 위해 설계한 모델에 기반한다[2]. 이 정책은 시스템에 있는 주체(subject)와 객체(object)의 분류등급(classification)에 따라 접근을 통제한다. 주체와 객체의 보안 등급(security level)은 TopSecret(TS), Secret(S), Confidential(C), 그리고 Unclassified(U) 등으로 되어 있고 TS ≥ S ≥ C ≥ U의 관계가 있다. 이 접근 제어 정책은 두 가지 기본적인 규칙을 정의하고 있다. 첫째는 주체는 자신의 접근 등급 이하인 객체만을 판독할 수 있다는 것과 둘째, 주체는 자신의 접근 등급 이상인 객체만을 기록할 수 있다는 것이다. 이 정책은 주로 시스템 데이터와 사용자가 등급화된 환경에서 강력한 보호가 필요한 대량의 정보에 적용되며, 트로이 목마나 비밀 채널(covert channel)과 같은 방법에 의한 데이터 침입을 보호하도록 설계되었다. 그러나 접근 권한 전달에 대하여, 할당된 권한은 바꿀 수 없으며 권한 관리자만이 수정할 수 있다. 이 의미는 권한부여 시스템에서 전적인 제어는 권한 관리자만이 한다는 뜻이다. 관계형 데이터 베이스 보호를 위한 강제적 보안 모델(mandatory security model)로는 보안 분류 등급을 고려한 정형화된 관계형 모델을 제안한 Jajodia-Sandhu 모델, 신뢰적인 이론에 기초한 모델을 제안한 Smith-Winslett 모델, MAC과 DAC 정책을 통합하여 제안한 Sea View 모델 등이 있다[7-10].

2.2 DAC Policy

임의적 접근 제어 정책은 사용자의 정체성(identity)과 규칙에 의거해서 정보에 대한 접근을 통제한다. 한 사용자가 다른 사용자에게 객체에 접근할 권한을 허가(grant)해 줄 수 있다는 면에서 임의적이라 할 수 있다[3]. 이 정책의 유연성 때문에 대부분의 기존 DBMS들은 이 정책을 적용하

여 접근 제어를 시행한다. 그러나 이 정책은 다른 사용자에게 접근 권한을 데이터의 소유자 모르게 넘겨 줄 수 있기 때문에, 프로그램에 내재된 트로이 목마와 같은 악의적인 공격에 취약하다. 관계형 데이터 베이스 보호를 위한 임의적 보안 모델(discretionary security model)로는 Wood 등이 제안한 모델이 다단계 스키마 관계형 데이터베이스에서의 권한 부여 문제를 고려한 것이다[6].

2.3 RBAC Policy

역할 기반 접근 제어 정책은 사용자가 적절한 역할에 할당되고 역할에 접근권한이 할당된 경우에만 사용자가 특정한 모드로 정보에 접근할 수 있다[4, 5]. 역할간의 계층관계는 접근권한의 상속이 이루어질 수 있도록 유지되어야 하고 역할의 특성에 따라 임무분리를 요하는 보안정책이 규정되어야 한다. 이 정책은 보안 관리를 아주 단순하게 할 수 있도록 하며, 사용자에게 최소의 권한만을 허용하여 권한의 남용을 방지한다. 그러나 이 정책이 대규모 시스템에 적용되었을 경우 많은 역할과 역할 허가 사이의 복잡한 관계 설정으로 실제 시스템을 완전히 통제하지는 못한다. 이 정책은 Sandhu-Bhamidipati, Ferraiolo 등에 의해 이 정책에 대한 변형 및 새로운 주제(issue)에 관한 연구가 진행중에 있다[11, 12].

3. 사용자 및 데이터 정의

3.1 사용자

사용자는 정보 접근의 주체(subject)로서 데이터베이스의 사용자 또는 사용자 그룹을 의미하며, 다음과 같이 정의한다.

- 사용자 집합 $U=\{u_1, u_2, u_3, \cdots, u_p\}$, p는 사용자 수
- 사용자 부분집합 $S=\{S_1, S_2, S_3, \cdots, S_t\}$, $S_q \subset U$, t는 사용자 부분집합의 수
- 보안 등급에 의한 사용자 그룹 $H=\{H_1, H_2, H_3, \cdots, H_m\}$, m은 보안 등급의 수
- 역할에 의한 사용자 그룹 $R=\{R_1, R_2, R_3, \cdots, R_n\}$, n은 역할의 수
- $u_i \in H_k$, $u_i \in R_l$
- $1 \le N(H_k) \le p$, $1 \le N(R_l) \le p$, $N(\cdot)$는 전체 사용자의 수

위에서 기술한 보안 등급은 조직체에서의 사용자의 위치와 업무에 따라 Admin, T1, T2, T3로 구분하였으며, Admin ≥ T1 ≥ T2 ≥ T3의 관계를 갖는다. 예를 들어 T1의 등급은 세부책임자에게 부여된다.

3.2 데이터

데이터는 정보의 집합을 나타내는 객체(object)로서 하나의 데이터 또는 데이터 그룹으로 정의한다. 그룹화는 크게 두 가지 기준에 준한다. 첫째, 모든 데이터는 속성 이름(attribute name)을 기준으로 하여 보안 등급으로 그룹화한다. 둘째, 데이터는 테이블 이름(table name), 속성 이름(attribute name)과 레코드 키(record key)에 의하여 다양한 크기로 그룹화 되며, 이때 레코드 키는 원하는 레코드를 식별할 수 있는 포괄적인 정보를 의미한다. 이 방법에 의한 데이터 그룹은 다음과 같이 정의한다.

- $DG=\{DG_1, DG_2, DG_3, \cdots, DG_n\}$, n은 데이터 그룹 수

  $DG_i=\{Table\ Name, Attribute\ Name(s), Record\ Key(s)\}$

위의 정의에 따라, 데이터 그룹은 다음과 같이 서로 다른 세 가지 유형을 갖는다.

① 테이블 전체 : $DG_i^1=\{Table\ Name, NULL, NULL\}$

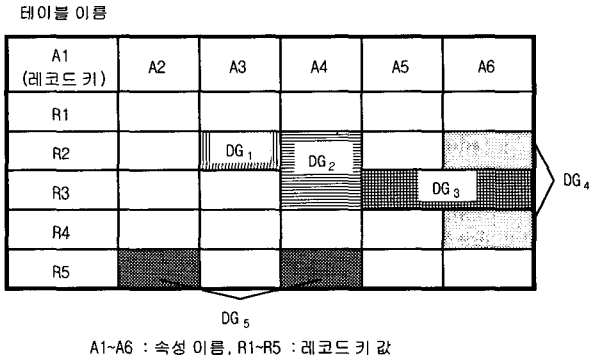
② 테이블과 속성 :

$DG_i^2=\{Table\ Name, Attribute\ Name(s), NULL\}$

③ 테이블, 속성과 레코드 키 :

$DG_i^3=\{Table\ Name, Attribute\ Name(s), Record\ Key(s)\}$

첫 번째 유형인 DG_i^1은 테이블 전체를 하나의 데이터 그룹으로 설정하며, 두 번째 유형인 DG_i^2은 특정 테이블의 속성(들)으로 데이터 그룹이 정의되고, 세 번째 유형인 DG_i^3은 두 번째 유형보다 작고 다양한 크기의 데이터 그룹을 표현할 때 사용하는데, 테이블 이름, 속성 이름, 레코드 키의 조합으로 한 개 이상의 데이터 항목에 대하여 그룹으로 설정한다. (그림 1)은 세 번째 유형의 데이터 그룹의 예이다.



(그림 1) DG_i에 의한 데이터 그룹

(그림 1)에서와 같이 데이터 그룹 $DG_1\{Table\ Name, A_3, R_2\}$으로 표현되는 하나의 데이터 항목을 나타내며, 다른 데이터 그룹들은 다음과 같이 표현된다.

$DG_2=\{Table\ Name, A_3, \{R_2, R_3\}\}$,

$DG_3=\{Table\ Name, \{A_5, A_6\}, R_3\}$

$DG_4=\{Table\ Name, A_6, \{R_2, R_4\}\}$,

$DG_5=\{Table\ Name, \{A_2, A_4\}, R_5\}$

4. 보안 요구사항

본 논문에서 제안하는 시스템은 다음과 같은 보안 정책을 만족하도록 설계되었다. 제시한 보안 정책들은 특정 유전체 연구 센터의 정보에 보안 관리를 효율적으로 하기 위한 요구사항을 반영하고 있다. 다음에서 제시한 정책들에서 $SL(\cdot)$은 보안등급을 나타낸다.

[정책 1]

$SL(H_k) \geq SL(DG_i^2) \rightarrow \{u_i \in H_k, DG_i^2, \{R, I, U, D\}\}$

사용자 u_i는 사용자 그룹의 보안 등급이 데이터 그룹의 보안 등급을 지배하면 DG_i^2의 데이터 그룹에 대하여 read(R), insert(I), update(U), delete(D) 할 수 있다.

[정책 2]

$\{u_i \in \{R_c \rightarrow DG_i^2\}\} \rightarrow \{u_i \in R_c, DG_i^2, \{R, I, U, D\}\}$

사용자가 u_i가 $u_i \in R_c$이고 R_c에 속할 경우 R_c에 할당된 DG_i^2의 데이터 그룹에 대하여 read(R), insert(I), update(U), delete(D)할 수 있다.

[정책 3]

위의 보안 정책을 만족할 경우, 특정 사용자만이 특정 그룹으로 정의된 데이터에 대하여 *read* 할 수 있다.

위의 보안 정책을 만족하기 위하여 접근 제어는 2단계에 의하여 이루어진다. 제 1단계에서는 MAC과 RBAC의 조합에 의하여 사용자가 요구한 질의문의 수행여부를 결정한다. MAC 정책의 응용으로 주체의 보안 등급이 객체의 보안 등급을 지배하면 네 가지 모드(read, insert, update 및 delete)를 수행할 수 있다. MAC 정책의 단점은 하위 주체가 상위객체에 네 가지 모드를 수행할 수 있으므로 데이터 무결성이 보장되지 않는 반면, 본 논문에서는 하위 주체가 상위 객체에 네 가지 모드를 허용하지 않도록 하여 데이터 무결성을 보장하였다. 또한, RBAC 정책의 응용으로 특정 역할을 할당 받은 사용자는 역할에 할당된 데이터를 네 가지 모드로 수행할 수 있도록 하여 필요에 따라 보안 등급이 낮을지라도 높은 등급의 데이터를 접근할 수 있도록 하였다. 이 단계에서 insert, update, delete 모드 수행에 대한 접근 제어가 완성된다. read 모드에 대한 접근 제어는 단계적으로 수행된다. 제 1단계에서 모든 사용자는 보안 등급과 역할에 의해 데이터에 대한 접근제어가 이루어진다. 즉, read 모드에 대한 접근 제어가 수정된 MAC과 RBAC 정책에 따라 오직 역할과 보안 등급에 의해서만 수행된다. 제 2단계에서는 위의 정책 3을 위한 DAC 정책의 응용으로서, read 모드에 대하여 작은 수의 데이터 항목으로 구성된 데이터 그룹에 대하여 세부적으로 접근 제어가 이루어진다. 즉, 1단계 read 모드의 수행 결과에 대하여 특정 사용자가 다양한 크기의 특정 데이터 그룹에 대한 read를 허용하지 않도록 한다. 또한, 임의의 사용자가 다른 사용자에게 특정 데이터에 대한 권한을 임의적으로 허가할 수 없도록 하여 DAC의 단점을 보완하였다. 데이터 그룹에 대한 접근 정책은 ***Block*(s, d, r)** 로 표현되며, 다음과 같다.

- ***Block*(s, d, r)**
  $s \in S_j, j = \{1,2,\cdots,u\}, u$는 특정 사용자그룹의 수
  $d \in DG_r, r = \{1,2,\cdots,v\}, v$는 데이터그룹의 수
  r : read mode

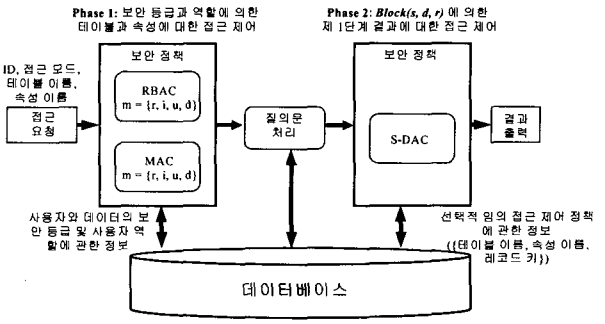
예를 들어, ***Block*(S_l, DG_q, r)** 접근 제어 정책은 S_l에 속한 사용자는 DG_q의 데이터 그룹에 대하여 read 할 수 없음을 의미한다. 이와 같이 제 2단계에서는 ***Block*(s, d, r)** 정책을 설정함으로써 사용자에 대하여 다양한 크기의 데이터 그룹에 대한 read 모드 접근 제어를 수행한다. 또한, 사용자에 대한 접근 제어 요구에 따라 ***Block*(s, d, r)** 정책을 설정할 수 있도록 하여 접근 제어 요구사항이 수시로 변하는 상황에 유연하게 대처할 수 있다.

5. 시스템 구조 및 기능

본 장에서는 앞에서 기술한 정의 및 보안 정책을 기반으로 제안한 세부 접근 제어 시스템 구조와 시스템을 구성하는 모듈의 기능에 관하여 기술한다. 또한, 세부적인 read 모드에 대한 접근 제어 시스템의 구현 결과를 기술하고자 한다. 제안한 시스템은 관계형 데이터베이스 Oracle 9i에 적용함으로써 기존의 데이터베이스 시스템의 접근 제어 기능을 확장하였다.

5.1 시스템의 구조

보안관리자는 사용자 그룹 S_c, H_j와 R_j 테이블과 속성들에 대한 보안 등급, 역할 부여, 데이터 그룹 DG_j와 ***Block*(s, d, r)** 정책들을 생성 및 저장한다. 이러한 정보들은 시스템을 구성하고 있는 모듈들의 수행을 위해 사용된다. (그림 2)는 전체 시스템의 구조를 보인다.



(그림 2) 시스템 구조

제 1단계에서는 먼저 접근하고자 하는 사용자 id를 검사하여 접근 요청이 SQL 문장 또는 역할에 의한 것인지를 파악한다. 만약, 접근 요청이 SQL 문장에 의할 경우 접근 모드, 테이블 이름, 속성들이 질의 문에서 추출되어 4장에서 기술한 정책1에 의해, 새로운 질의문이 생성된다. 또한, 역할에 의할 경우 사용자의 역할에 따른 접근 권한이 검사되고 할당된 접근 권한이 존재할 경우 RBAC 모듈이 수행된다. 접근 요청이 위의 정책들을 만족하지 않을경우 접근 요청은 거부된다. 제 2단계의 변형된 DAC정책은 작은 수의 데이터 항목으로 구성된 다양한 크기의 데이터 그룹에 대하여 접근 제어한다는 의미에서 선택적 DAC(Selective-DAC : S-DAC)정책이라 정의한다. 이 단계에서는 1단계에서 수행된 결과가 ***Block*(s, d, r)**에 의해 표현되는 정책 3에 따라 S-DAC에 의해 다양한 크기의 데이터 항목들이 선택적으로 필터링된다. 결과적으로 위의 정책들을 모두 만족하는 데이터 항목만이 사용자에게 보여진다.

5.2 모듈별 기능

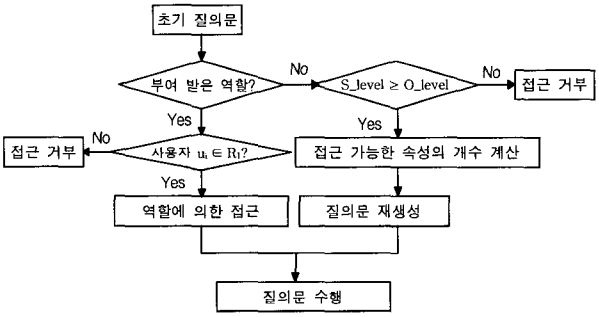
각 단계에서 접근 제어를 위해 사용되는 MAC 모듈, RBAC 모듈과 S-DAC 모듈의 상세한 기능 및 동작 흐름은 다음과 같다.

5.2.1 RBAC 모듈

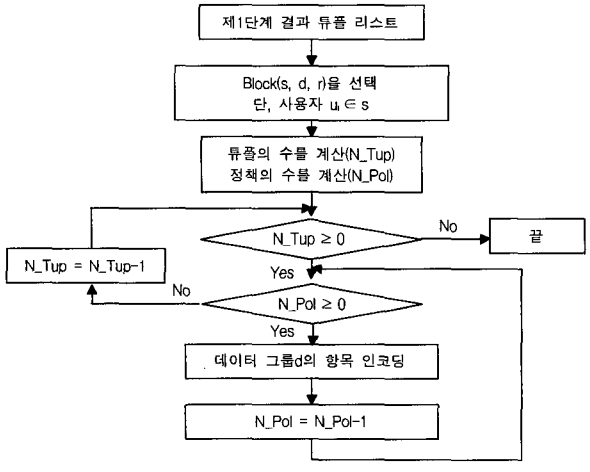
역할에 의한 접근 요청이 있을 경우, RBAC 모듈은 사용자가 속한 그룹을 파악하고 그 그룹의 역할을 식별하여 권한이 있는지를 비교한다. 만약, 사용자 $u_i(u_i \in R_l)$가 역할 R_l에 관한 접근 권한이 있다면 접근이 허용되고, 접근 권한이 없다면 접근은 거부된다.

5.2.2 MAC 모듈

SQL 질의문을 통해 접근 요청이 들어올 경우 MAC 모듈은 사용자 등급과 질의문의 테이블과 속성들의 보안 등급을 비교한다. 사용자 등급이 데이터의 등급을 지배하면 접근 가능한 속성들의 수를 계산하고, 접근 가능한 속성 이름을 추출한다. 이러한 과정의 처리 결과로 새로운 질의문이 생성되는데, 이는 4장에서 정의한 정책 1을 만족한다. (그림 3)은 MAC과 RBAC 모듈의 처리 과정을 보인다.



(그림 3) MAC과 RBAC 모듈 처리 순서도



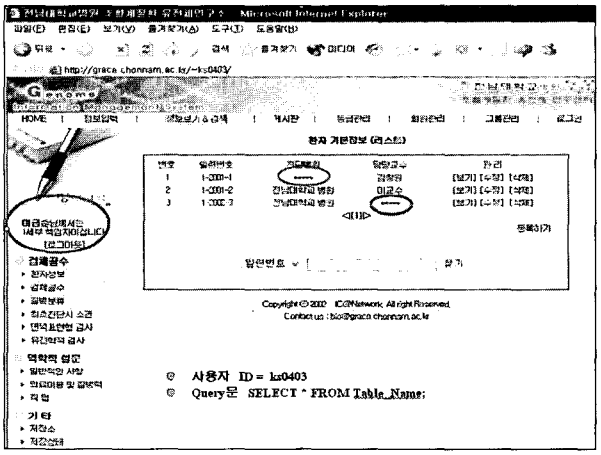
(그림 4) S-DAC 모듈 처리 순서도

5.2.3 S-DAC 모듈

세부적인 접근 제어는 MAC 모듈과 RBAC 모듈에 의한 1단계 접근 제어가 이루어진 후 실행된다. (그림 4)는 S-DAC 모듈의 처리 과정을 보인다. S-DAC 모듈은 사용자가 접근 요청한 테이블에 대하여 S-DAC 정책 즉 ***Block*** ***(s, d, r)*** 들의 수를 파악하고, 이 정책에 의해 설정된 데이터 그룹들을 검사한다. 이와 같이 ***Block(s, d, r)*** 정책을 반영하여 s, d, r항목이 모두 만족하는 경우 1단계 결과의 튜플 리스트에 대하여 데이터 그룹으로 설정된 데이터 항목 값들이 보여지지 않는다.

5.3 구현 결과

(그림 5)는 보안등급 T2인 선임연구원이 질의문 "SELECT*FROM Patient_Info ; "을 요청할 경우, 실행된 결과 화면을 나타낸다. 이 선임연구원은 원래 환자정보 테이블(patinet_Info)에 대한 read 모드 접근 권한이 있으나, 조직체의 특정 보안정책에 따라 특정 데이터 항목에 대한 read 모드 접근을 할 수 없도록 한 상태이다. 결국, 이러한 사용자는 환자 '1-2001-1'에 대한 'Diagnosis Hospital' 정보와 환자 '1-2002-3'에 대한 'Doctor'정보에 대한 read 모드 접근은 할 수 없다는 것을 알 수 있다. 이러한 결과는 ***Block(s, d, r)*** 정책에 의한 것이며, 정책의 수행 결과 값들은 '*****' 문자로 대체되도록 하였다.



(그림 5) 시스템 구현 및 질의문 실행 결과

6. 결 론

데이터베이스의 규모가 커지고, 데이터베이스를 이용하는 사용자들의 요구가 복잡하고 다양해지면서 데이터베이스 보안의 중요성이 커졌다. 많은 데이터베이스 보안 모델들이 존재하지만 데이터베이스 보안 정책이 수시로 바뀌고, 특정 사용자의 다양한 크기의 데이터 항목들에 대해 각각 다른 접근 제어를 필요로 하는 등의 요구사항을 수용하지 못한다. 본 논문에서는 이를 해결하고자 기존의 보안 정책인 MAC, DAC, RBAC 등을 조합 및 변형하여 세부적 접근 제어를 위한 시스템을 제안하였다.

제안한 시스템은 크게 두 단계로 나누어 보안 정책을 수행한다. 제 1단계에서는 수정된 MAC 정책과 RBAC 정책을 이용하여 보안 등급과 역할에 따라 접근 제어가 이루어진다. 제 2단계에서는 S-DAC 정책을 이용하여 테이블과 속성단위보다 작은 크기의 데이터 그룹에 대하여 read 모

드에 대한 접근 제어를 수행한다. 즉, 1단계에서의 질의문 수행결과에 대하여 특정 사용자가 특정 데이터를 read 할 수 없도록 하였다. 이와 같이 제안한 시스템은 각 사용자에 대하여 다양한 크기의 데이터 항목들에 대한 read 접근 제어를 가능하게 하여 복잡한 사용자의 접근 요구를 수용하고, 접근제어 요구사항이 변하는 상황에 쉽게 대처할 수 있다. 제안한 시스템은 사용자별 데이터에 대한 접근 제어가 복잡하게 요구되는 특정 유전체 연구 센터의 정보에 보안 관리를 위해 사용하였다.

제안한 보안 관리 시스템은 각 사용자별로 다양한 크기의 데이터 그룹에 대한 read 접근 제어를 유연하게 제공한다. 그러나, 데이터 그룹을 정의하는 과정에서 대량의 레코드 키값을 구하기 위한 오버헤드가 클 수 있다. 또한, 새로운 접근 제어가 필요할 경우 정책을 추가 생성하므로 ***Block(s, d, r)*** 정책 수의 증가에 따라 시스템의 성능을 저하시킬 우려가 있고, 같은 사용자에 따른 정책들의 중복 현상이 나타날 수 있다. 그러므로 시스템의 성능을 보다 향상시키기 위해 레코드 키 값을 구하기 위한 오버헤드를 줄이는 방법과 같은 사용자에 대하여 ***Block(s, d, r)*** 정책들을 통합하고 재정의함으로써 정책을 감소할 수 있는 방법이 향후 연구되어야 할 것이다.

참 고 문 헌

[1] M. Piattini and E. Fernandez-Medina, "Secure databases : state of the art," Security Technology, Proc. Of the IEEE 34th Annual 2000 International Carnahan Conference, pp. 228-237, 2000.

[2] R. Lindgreen and I. Herschberg, "On the Validity of the Bell-LaPadula Model," Computer & Security, Vol.13, pp. 317-338, 1994.

[3] S. Lewis and S. Iseman, "Securing an object relational database," Computer Security Applications Conference, 1997.

[4] D. Ferraiolo, R. Sandhu, S. Gavrila, D. Kuhn and R. Chandramouli, "Proposed NIST Standard for Role-Based Access Control," ACM Transactions on Information and Systems Security, Vol.4, No.3, pp.224-274, Aug., 2001.

[5] R. Sandhu, E. Coyne, H. Feinstein and C. Youman, "Role-based access control models," IEEE Computer, Vol.29, Issue 2, pp.38-47, 1996.

[6] C. Wood, R. Summers, and E. Fernandez, "Authorization in multilevel database models," Information Systems, Pergamon Press, 4(2), 1979.

[7] S. Jajodia and R. Sandhu, "Enforcing primary key requirements in multilevel relations," In Proc. 4th RADC Workshop on Multilevel Database Security, Little Compton, Rhode Island, 1991.

[8] R. Sandhu and S. Jajodia, "Polyinstantiation for cover stories," In Proc. European Symposium on Research in Computer Security, Toulouse, France, Springer-Verlag LN CS 648, 1992.

[9] M. Winslett, K. Smith and X. Qian, "Formal query language for secure relational databases," ACM-TODS, 1994.

[10] D. Denning et al., "The Sea View Security Model," In Proc. IEEE Symp. on Security and Privacy, Oakland, CA, pp.218-233, 1988.

[11] R. Sandhu and V. Bhamidipati, "The URA97 model for role-based user-role assignment," Database Security XI : Status and Prospects, Chapman and Hall, London, pp.262-275, 1997.

[12] D. Ferraiolo, J. Barkley and R. Kuhn, "A role-based access control model and reference implementation within a corporate intranet," ACM Transactions on Information and Systems Security, Vol.2, No.1, pp.34-64, 1999.

정 민 아

e-mail : majung@grace.chonnam.ac.kr
1992년 전남대학교 전산통계학과(학사)
1994년 전남대학교 대학원 전산통계학과 (이학석사)
2002년 전남대학교 대학원 전산통계학과 (이학박사)
2002년~2003년 광주과학기술원 정보통신학과 Post-Doc.
2003년~현재 전남대학교 전자통신기술연구소 Post-Doc.
관심분야 : 생물정보학, 데이터마이닝, 정보보호, 데이터베이스,

김 정 자

e-mail : jjkim@grace.chonnam.ac.kr
1985년 전남대학교 전산통계학과(학사)
1988년 전남대학교 대학원 전산통계학과 (이학석사)
2002년 전남대학교 대학원 전산통계학과 (이학박사)
2002년~현재 전남대학교 전자통신기술 연구소 Post-Doc.
관심분야 : 생물정보학, 데이터마이닝, 데이터베이스, 정보보호

원 용 관

e-mail : ykwon@grace.chonnam.ac.kr
1986년 한양대학교 전자공학과(학사)
1991년 Univ. of Missouri, 컴퓨터공학과 (공학석사)
1995년 Univ. of Missouri, 컴퓨터공학과 (공학박사)
1991년~1995년 Univ. of Missouri, Research/Teaching Assistant
1995년~1996년 전자통신연구원
1996년~1999년 한국통신 연구개발본부
1999년~현재 전남대학교 컴퓨터공학과 부교수
관심분야 : 패턴인식, 데이터마이닝, 생물정보학, 네트워크 관리 및 보안

배 석 찬

e-mail : scbae@kunsan.ac.kr
1983년 전남대학교 계산통계학과(이학사)
1988년 전남대학교 대학원 전산통계학과 (이학석사)
1995년 전남대학교 대학원 전산통계학과 (이학박사)
1983년~1985년 ROTC
1993년~1994년 서남대학교 전산통계학과 학과장
1995년~현재 군산대학교 컴퓨터정보과학과 부교수
관심분야 : 트랜잭션 관리, 데이터베이스 보안, 객체지향 시스템