□특집□

데이터베이스 시스템의 보안 기술

주 광 로† 박 우 근††

◈ 목 차 ◈

1. 서 론

급격한 정보화 추세에 따른 컴퓨터의 대량 보급과 통신망의 확대는 사용자의 편리성과 효율성을 극대화 시키며 국가 산업 경쟁력의 바탕이 되고 있으며, 이러한 정보화의 시대적 추세에 발맞추어 국내외적으로 초고속정보통신망 구축과 같은 다양한 연구가 진행 중에 있다. 초고속정보통신망의 구축은 전송 속도의 고속화, 대용량의 멀티미디어 정보 전송 등과 같은 긍정적인 효과를 거두고 있지만, 컴퓨터 시스템의 장애 또는 부정한 방법으로 피해를 유발시키는 컴퓨터 범죄와 개인의 사생활 침해, 그리고 컴퓨터 바이러스 등 역기능적인 부작용이 중요한 문제로 대두되고 있다.

정보 통신망에서 운영되는 정보를 저장 관리하는 컴퓨터 시스템에서 보안(security)의 필요성은 컴퓨터에서 처리되는 정보를 권한이 없는 사용자가 판독하거나 또는 부적절하게 기록하는 것을 방지하며, 그리고 정당한 권한을 갖는 사용자의 정보 처리 서비스를 컴퓨터 시스템에서 거부되지 않도록 보호하기 위한 것이다. 특히, 대용량의 자료를 보관하는 데이터베이스 관리 시스템에서는 데이터의 무결성(integrity), 기밀성(secrecy), 그리고 이용성(availability) 보장이 필수적으로 요구된다.

본 고에서는 데이터베이스 관리 시스템(database management system: DBMS)을 위협하는 보안성 위협의 요소들을 정리하고, 이에 대한 대책 수단을 살펴본다. 또한, 데이터베이스에서 보안성이 제공될 수 있도록 현재까지 관계형 DBMS와 객체지향 DBMS에 대해 연구 개발된 기본적인 보안 서비스인 접근 제어 기술에 대해 설명한다.

본 고의 구성은 다음과 같다. 먼저, 2장에서는 데이터베이스의 보안 위협 요소들을 정리하고, 이를 대처하기 위한 보안성 강화 방안들에 대해서 언급한다. 그리고 3, 4장에서는 각기 관계형 DBMS와 객체지향 DBMS에서 데이터의 보안성을 유지하기 위해 개발된 보안 모델들과 특징에 대해서 간략히 설명하고, 마지막으로 5장에서는 결론과 향후 연구 방향에 대해서 언급한다.

† 정회원 : 서강전문대학 전산과 교수
†† 정회원 : 광주대학교 전산학과 교수

2. DBMS 보안 요구사항 및 대책 수단

2.1 DBMS 보안 요구사항

데이터베이스 보안을 달성하기 위해서는 무엇보다도 DBMS에서 발생할 수 있는 여러 형태의 보안 위협 요소들의 식별이 필요하다. 우발적으로 혹은 특별한 기술을 사용하여 DBMS에서 관리하는 정보를 부적절하게 노출시키거나, 변경하는 악의가 있는 행위 모두가 위협 요소이며, 이는 세 가지 형태로 분류된다.

- 데이터의 노출(disclose)
- 데이터의 부적절한 수정(modification)
- 서비스의 거부(denial of service)

따라서, 데이터베이스의 보호는 DBMS의 자원인 저장된 데이터를 우발적 또는 의도적으로 권한이 없는 사용자가 판독 그리고 갱신하는 것을 방지하는 동시에 정당한 권리를 갖는 사용자가 부당하게 서비스의 거부를 당하지 않도록 함을 의미한다. 이를 위해 DBMS에서는 다음과 같은 보안 요구사항이 만족되어야 한다[13].

① 정당한 사용자의 데이터 접근 지원
② 추론 방지
③ 데이터 무결성 유지
④ 데이터 연산 무결성 유지
⑤ 데이터 의미(semantic) 무결성 유지
⑥ 시스템 감사(audit)
⑦ 사용자 인증(authentication)
⑧ 기밀 데이터 관리와 보호
⑨ 다단계 보호(multilevel protection)
⑩ 감금(confinement)

①은 DBMS의 정당한 권한을 갖는 사용자가 부당하게 서비스 거부되지 않기 위한 것이며, ⑥, ⑦,과 함께 DBMS의 가장 기본적인 보안 요구사항이다. 반면에, ③, ④, ⑤ 조건은 데이터의 논리적인 일관성 유지에 필요한 DBMS의 기초적인 조건이다.

그리고 보다 강력한 형태의 보안성이 요구되는 다양한 응용들을 지원하기 위해서 ②, ⑧, ⑨, ⑩과 같은 보안 요구사항이 DBMS에 존재하다.

2.2 보안 대책

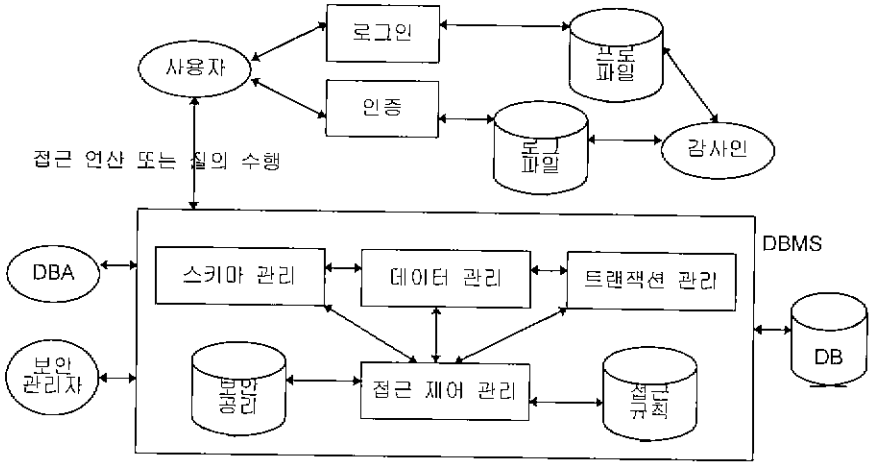
2.1절에서 언급한 DBMS 보안 요구사항을 만족시키기 위한 수단으로서 다음과 같은 세가지 방법이 널리 사용된다.

- 접근 제어(access control) 방법
- 정보 흐름 제어(flow control) 방법
- 추론 제어(inference control) 방법

첫번째 방법은 사용자가 데이터베이스에 직접적인 경로를 통해서 접근할 때, 이를 통제하여 데이터의 보안성을 달성하는 방법이다. 반면에, 세번째 방법은 데이터에 직접적인 접근으로 정보를 얻기보다는 간접접인 수단 즉, 추론 채널(covert channel) 또는 통계 추론 등으로 정보를 부당하게 접근하지 못하도록 통제하는 기술이다. 두번째 방법은 사용자가 접근할 수 있는 데이터들 사이에서 정보의 분배 또는 흐름이 발생할 때, 권한이 부여되지 않은 데이터 사이에서 부당한 데이터 전달을 통제하는 기술이다. 본 고에서는 대부분의 DBMS에서 채택하고 있는 일반적인 보안 수단인 접근 제어 기법과 이를 확장하여 정보의 흐름까지도 통제하여 강력한 보안성을 유지시키는 데이터베이스 시스템의 보안 모델들을 중심으로 설명한다.

DBMS에서 보안성을 유지하기 위한 구조는 (그림 1)과 같이 구성되며, DBMS에서 데이터 보호를 위해 수행하는 접근 제어 방법은 DBMS에 설정된 보안 공리와 접근 규칙과 같은 명시적인 규칙을 기반으로 수행한다.

접근 규칙과 보안 공리는 DBMS가 선택한 접근 제어 정책에서 유도되며, 대부분의 DBMS에서



(그림 1) 보안 DBMS의 구조

는 폐쇄 시스템 환경에서 널리 채택된 최소 권리 정책(minimum privilege policy)에 입각한 다음과 같은 두가지 형태의 접근 제어 정책을 사용한다.

- 자율적 접근 제어(discretionary access control: DAC) 정책
- 강제적 접근 제어(mandatory access control : MAC) 정책

사용자 또는 이들이 속한 그룹이 시스템의 인증 결과로 얻어진 식별자(identifier)에 근거하여 객체에 대한 접근을 제한하는 방법이 DAC 정책이다. 이 정책에서는 사용자가 특정 객체에 접근 권리를 갖는 한 자율적으로 다른 사용자에게 자신의 권리를 넘겨줄 수 있기 때문에 자율적 정책이라 하며, 대표적인 모델로는 접근 행렬(access matrix) 모델이 있다[6].

반면에, MAC 정책은 객체에 포함된 정보의 비밀성 또는 보안등급(classification)과 이러한 비밀 데이터의 접근 정보에 대하여 사용자가 갖는 권한 또는 인가등급(clearance)에 기초하여, 정의된 조건이 만족하는 경우에만 객체에 대한 접근을 허용하고, 또한 데이터의 흐름을 제어하는 방법이다. 이에 해당하는 대표적인 보안 모델로 BellLapadula (BLP)와 Biba 모델이 있다[2, 5].

3. 관계형 DBMS를 위한 보안 모델

관계형 DBMS에서 데이터의 보호는 2.2절에서 언급된 DAC 정책과 MAC 정책에 해당하는 보안 모델들을 기초로 하여, 이를 관계형 데이터베이스에 적합하도록 확장한 접근 제어 모델에 의해서 이루어진다.

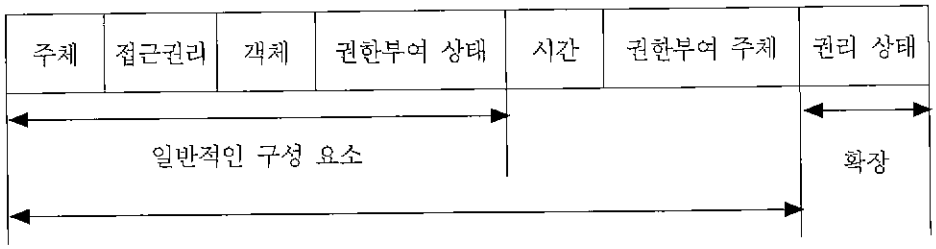
3.1 DAC 정책 기반의 관계형 DBMS 보호

관계형 DBMS에서 DAC 정책을 지원하기 위한 다양한 접근 제어 모델들이 개발되었으며, 대부분의 보안 모델들이 접근 행렬 모델을 기초로 하여, 관계형 데이터 모델의 구성 요소들에 DAC 정책의 보안 특성을 적용하고 있다. 관계형 DBMS의 대표적 접근 제어 모델은 IBM에서 개발한 System R의 접근 제어 모델이며[9], 현재 널리 사용되고 있는 관계형 DBMS들인 Ingres, Sybase, Informix 등에서도 유사한 모델을 사용하고 있다.

본 절에서는 System R 접근 제어 모델을 바탕으로 기본적인 접근 제어 방법과 확장된 개념의 접근 제어 기법을 설명한다.

3.1.1 기본 개념

DAC 정책을 기반으로 하는 DBMS에서 데이터에 대한 사용자의 접근 통제는 접근 규칙 데이터베이스에 저장된 접근 규칙을 바탕으로 이 사용자가 접근하려는 데이터에 접근 권리가 명시적으로 기술되었는지를 확인하므로써 수행된다. 따라서, 접근 제어 모델은 접근 규칙의 구조를 기술하고, 그리고 접근 규칙을 생성하고 삭제시키는 접근 규칙의 관리 방법이 정의되어야 한다. 일반적인 형태의 접근 규칙의 구조는 (그림 2)와 같다.



(그림 2) 접근 규칙의 구조

(그림 2)에서 앞의 4가지 요소들이 접근 제어 모델들에서 공통적으로 기술되는 접근 규칙의 구성 요소들이다. 주체는 데이터베이스를 접근하는 사용자 또는 프로세스이며, 접근 권리는 이 사용자가 데이터에 대해 수행한 SQL 데이터 연산의 형태이다. 또한, 객체는 관계형 데이터베이스 테이블이 대상이며, 기본(base) 테이블과 뷰(view) 테이블 모두가 해당한다. 권한부여 플레그는 주체가 자신이 갖는 접근 권리를 다른 사용자에게 부여할 수 있는권리를 기술한다. 특히, System R에서는 부가적으로 권한부여 시간과 권한부여 주체와 같은 2가지 요소를 포함하고 있다. 시간은 접근 규칙이 생성된 때를 의미하고, 권한부여 주체는 이 접근 규칙의 주체에게 접근 권리를 부여한 사용자를 나타낸다.

대부분의 접근 제어 모델에서 접근 규칙을 생성하고 삭제시키는 관리 방법은 소유권(ownership) 정책에 입각하여 수행된다. 따라서, DBMS 사용자는 누구라도 새로운 테이블과 뷰를 생성할 수 있는 권리를 갖으며, 사용자가 테이블을 생성하는 경우에 그 사용자는 그 테이블에 대해 모든 형태의 접근 권리를 갖는다. 또한 테이블의 소유자는 접근 권리를 다른 사용자에게 부여할 수 있다. 만일 특정 사용자에게 권한부여가 이루어지면 이 사용자를 위한 접근 규칙이 DBMS에서 관리하는 접근 규칙들의 집합인 데이터베이스에 새롭게 생성된다. 이러한 접근 규칙의 관리를 위해서 접근 규칙을 생성하고, 삭제시키는 인터페이스를 DBMS가 제공하며, 이는 기존의 SQL 언어를 확장시켜 제공한다.

3.1.2 권한의 철회

DBMS가 유지하는 접근 규칙 데이터베이스에서 특정한 접근 규칙을 삭제시키는 것은 특정 사용자에게 부여된 접근 권리를 철회하므로써 수행되며, 이때 사용되는 방법으로 순환적 철회(cascading revoke)와 비순환 철회 방법이 있다.

순환적 철회 방법에서는 사용자 y에게서 특정

테이블 t에 대한 권리 p를 사용자 x가 철회하면 그 결과는 y에게 x에 의해 t에 대해서 부여된 p가 결코 부여되지 않은 상태로 접근 규칙 데이터베이스가 복구된다. 따라서, 특정 권리를 철회하면 다른 사용자에게 접근 권한을 부여한 규칙들 또한 모두 연쇄적으로 제거되는 효과를 갖는다.

그러나 대부분의 데이터베이스 응용들에서는 하나의 사용자가 데이터베이스에 대해 소유하는 권한은 사용자가 응용에서 자신의 작업을 수행할 때 필요한 것이며, 만일 이 사용자의 작업 영역이 바뀌는 경우에 사용자가 다른 사용자에게 부여한 권한을 철회시키지 않고, 이 사용자의 권한만 철회해야 한다. 따라서, 이런 환경에서 순환적 철회 방식은 문제가 있으며, 이를 해결하기 위해서 비순환적(non-cascading) 철회 방식이 사용된다. 비순환적 철회는 권한을 철회할 사용자가 다른 사용자에게 부여한 권한은 철회시키지 않고, 그 사용자에게 주어진 권한만 철회하는 방법이다[4].

3.1.3 내용 기반 접근 제어

관계형 DBMS에서 접근 제어 방법은 대부분이 명시적인 접근 규칙에 기초한 문맥 기반(context based) 보안을 시행하고 있으나, 데이터 내용(content)에 기반한 접근 제어를 시행할 수 있다. 이는 대부분의 관계형 DBMS에서 사용자가 데이터베이스에 존재하는 테이블에서 새로운 뷰 테이블을 유도할 수 있는 기능을 제공하기 때문에 가능하다. 예를 들어, 사용자 A가 하나의 테이블 T를 생성하고, T의 속성 p의 값이 1000이하인 튜플들에 대해서만 사용자 B에게 read 권리를 주고자 하는 경우에, A는 기본 테이블 T에서 속성 p의 값이 1000이하인 튜플만을 갖는 하나의 뷰를 정의한 후, 이 뷰에 대해서 read 권리를 B에게 부여하면 내용 기반 접근 제어가 시행될 수 있다.

뷰를 유도한 기본 테이블에 대해서 뷰의 생성자가 갖는 접근 권리가 뷰에 대해서도 동일하게 적용되며, 그리고 뷰 테이블도 기본 테이블과 마찬가지로 다른 사용자에게 권한부여가 이루어질 수 있다.

3.1.4 부정적 권한부여

System R과 유사한 관계형 DBMS의 접근 제어 모델에서는 폐쇄 보안 정책을 기반으로 하기 때문에, 사용자가 데이터베이스 테이블에 접근할 때 접근 규칙 데이터베이스 또는 시스템 카탈로그에 접근 규칙이 존재하지 않으면 사용자의 접근이 거부된다. 예를 들어, 사용자 A가 테이블 T에 대해서 read하지 못하도록 T에 대한 A의 read 권리를 정의한 접근 규칙을 생성하지 않으면 된다. 그러나 사용자 B가 T에 대해서 read 권리를 갖고서, 이를 A에게 권한부여를 시행하면 결과적으로 A는 T에 대해서 read 할 권리를 갖는다.

이러한 현상은 접근 규칙의 관리가 소유권 정책을 기반으로 하기 때문에 발생하며, 이런 경우에 기존의 접근 제어 모델에서는 이 사용자가 테이블을 접근하는 것을 방지할 수 없다. 부정적 권한부여(negative authorization)의 개념[4]은 이를 극복하기 위한 것이며, 사용자가 테이블에 대해 접근 권리를 갖지 않는다는 사실을 기술한 부정적 접근 규칙을 생성하는 것이다. 따라서, 사용자가 테이블에 접근하고자 할 때 DBMS는 이를 기반으로 테이블에 대한 접근을 거부하며, 그리고 다른 사용자가 동일 테이블에 대해서 권한을 부여하려 할 때, 이미 이 사용자에 대한 부정적 접근 규칙이 존재하기 때문에 권한부여는 수행되지 않는다.

3.2 다단계 보안(Multilevel Security) 관계형 모델

MAC 정책을 관계형 DBMS에 적용한 접근 제어 모델은 데이터베이스의 테이블과 튜플, 그리고 필드에 데이터의 기밀 정도를 나타내는 보안등급을 결합시키는 방법을 사용하고 있다(그림 3).

DAC 정책을 지원하는 관계형 DBMS에서 한 튜플의 필드 값은 단일 값인 반면에 MAC 정책을 시행하는 접근 제어 모델에서 한 튜플의 필드 값은 보안등급의 수준에 따라 다중 값을 갖을 수 있다. 따라서, 데이터 값이 단일 수준이 아닌 다단계로 구성되기 때문에 MAC 정책을 시행하는 보안 모델을 다단계 보안 모델이라 한다.

CL : Classification, TC : Tuple Classification

Name	Salary	Name	CL	Salary	CL	TC
Stallone	1000$	Stallone	U	1000$	U	U
Jeniffer	2000$	Jeniffer	U	2000$	U	U
Arnold	2500$	Jeniffer	U	4000$	S	S
		Arnold	S	3000$	S	S

(a) 단일 값 릴레이션 (b) 다단계 릴레이션

(그림 3) 단위 릴레이션 vs. 다단계 릴레이션

관계형 DBMS를 위한 여러 형태의 다단계 보안 모델들[7, 8]이 제안되고 있으나, 본 절에서는 대표적인 다단계 보안 모델인 Stanford 연구소에서 개발한 SeaView 모델을 바탕으로 다단계 보안 모델에서 중요한 개념인 다단계 릴레이션, 다단계 보안 공리 및 제약조건, 그리고 다중인스턴스화(polyinstanciation) 등에 대해서 설명한다.

3.2.1 다단계 보안 모델의 기본 구성

관계형 DBMS의 다단계 보안 모델인 SeaView는 MAC 정책을 시행하여 데이터 접근을 통제하는 MAC 모델과 다단계 릴레이션의 정의와 데이터의 보안등급을 결정하는 TCB(Trusted Computing Base) 모델로 구성된다.

MAC 모델의 구성[7]은 주체, 객체, 접근 권리, 보안등급(classification), 그리고 보안 공리(security axioms)로 이루어진다. 이 모델에서 두드러진 특징은 보안등급의 형태와 보안 공리이며, 보안등급은 BLP와 Biba 모델의 보안등급과 무결성 등급을 통합한 구조를 갖는다.보안 공리는 사용자가 데이터에 접근할 때 데이터의 보안성을 유지시키는 정보의 흐름이 발생하도록 제어하기 위한 것이며, 데이터의 판독, 기록 그리고 내장 프로시쥬어의 수행에 대한 보안성 제약조건을 기술한다.

다단계 보안 모델의 보안 공리는 모델별로 제약 조건이 상이하며, 이는 보안 모델이 BLP 모델을 지원하는냐 또는 Biba 모델을 지원하느냐, 혹은 통합된 보안 모델을 지원하느냐에 따라서 각기 다르게 결정된다.

3.2.2 다단계 릴레이션

다단계 릴레이션은 기존의 단위 릴레이션이 여러 수준의 보안등급을 포함하도록 확장시킨 구조이며 (그림 3b), 튜플의 모든 항목과 튜플 전체에 대한 보안등급이 결합된 형태를 갖는다. 이러한 다단계 릴레이션에는 이 릴레이션이 MAC 정책에 위배되지 않도록 반드시 만족해야 하는 여러 형태의 무결성 제약조건들이 다단계 보안 모델별로 다양하게 정의되고 있으며, 궁극적으로는 아래와 같은 두가지 종류의 목적을 달성하기 위한 제약조건들이다.

- 다단계 개체(multilevel entity) 무결성
  주키(primary key)를 구성하는 속성들의 값은 어떤 튜플 내에서도 동일한 보안등급을 갖으며, 주키 속성 값의 보안등급은 튜플에 존재하는 다른 모든 속성들 값의 보안등급에 의해 지배(dominate)된다.
- 다단계 참조(multilevel referential) 무결성
  다단계 릴레이션에서 특정 보안등급의 수준에서 접근할 수 있는 외래 키가 존재하면, 참조되는 주키를 포함하는 튜플 또한 그 보안등급에서 반드시 접근해야 한다.

3.2.3 다중인스턴스화

다단계 보안이 지원되지 않는 관계형 데이터베이스에서 각각의 튜플들이 주키의 값에 의해 유일하게 식별할 수 있으나, MAC 정책이 지원되는 관계형 DBMS에서는 주키 속성의 값이 동일하지만

키 값의 보안등급이 서로 다른 여러 개의 튜플들이 동시에 존재할 수 있다. 이와 같은 경우를 다중인스턴스화라 하며, 다중인스턴스화는 서로 다른 보안등급을 갖는 사용자들이 하나의 다단계 릴레이션에 대해서 연산을 수행할 수 있기 때문에 발생한다. 예를 들면, 한 사용자가 특정 릴레이션에 새로운 데이터를 추가하는 경우에 그 릴레이션에 동일한 값을 갖는 데이터가 높은 보안등급으로 이미 존재할 때 이 연산을 철회하지 못한다. 그 이유는 낮은 수준의 보안등급을 갖는 사용자가 높은 등급의 보안등급을 갖는 데이터가 존재한다는 사실을 추론할 수 있기 때문이며, 이러한 경우에 새로운 데이터의 삽입 연산을 허용하는 동시에 그 데이터에 대해 다중인스턴스화를 발생시킨다.

관계형 DBMS에서 발생하는 다중인스턴스화의 종류는 튜플 다중인스턴스와 속성 다중인스턴스화가 있으며, 튜플 다중인스턴스화는 (그림 4a)와 같이 동일한 주키 값을 갖지만 주키에 결합된 보안등급이 서로 다른 튜플들의 집합이 생성될 때 발생한다. 반면에 속성 다중인스턴스화는 주키 값과 주키에 결합된 보안등급이 동일하지만, 키가 아닌 다른 속성의 값에 결합된 보안등급이 서로 다른 튜플들의 집합이 생성될 때 발생한다(그림 4b).

Name	CL	Salary	CL	TC
Stallone	U	1000$	U	U
Jeniffer	U	1500$	U	U
Arnold	*S*	*2000$*	*S*	*S*
Arnold	*TS*	*4000$*	*TS*	*TS*

(a) 튜플 다중인스턴스화

Name	CL	Salary	CL	TC
Stallone	U	1000$	U	U
Jeniffer	*S*	*1500$*	*S*	*S*
Jeniffer	*S*	*3000$*	*TS*	*TS*
Arnold	TS	4000$	TS	TS

(b) 속성 다중인스턴스화

(그림 4) 다중인스턴스화의 형태

4. 객체지향 DBMS의 보호 기술

DBMS에서 보안을 유지하는 경우에는 보호할 데이터베이스 정보의 단위(granularity)와 데이터들 간에 존재하는 관계와 의미(semantics) 등을 고려해야 한다. 객체지향 DBMS는 관계형 DBMS와는 달리 복잡한 구조적 특징을 갖는 객체지향 데이터 모델을 제공할 뿐만 아니라 객체들 사이에서 복잡한 상호 관계를 표현하는 풍부한 의미적 특성을 갖는다. 따라서, 관계형 DBMS를 위한 접근 제어 모델들이 새로운 데이터 모델의 의미적 구조인 객체, 클래스, 메소드(method), 계승(inheritance), 그리고 캡슐화(encapsulation) 등에 대한 보안성을 만족시킬 수 없기 때문에 객체지향 데이터베이스에 적합하도록 기존의 접근 제어 모델을 확장하거나 또는 새로운 모델의 개발이 필요하다. 따라서, 본 장에서는 객체지향 DBMS에서의 접근 제어 기술에 대해서 설명한다.

4.1 객체지향형 접근 제어 모델

DAC 정책을 지원하는 객체지향 DBMS의 접근 제어 모델은 사용자의 접근으로 부터 통제할 대상이 무엇이냐에 따라 2가지 부류로 구분한다. 구분의 기준은 객체지향 DBMS에서 지원하는 보안성이 고려되지 않은 데이터 모델의 모습에서 기인한 것이며, Gemstone, Versant, O2, UniSQL 등과 같은 상용 DBMS는 첫번째 방법을 사용한다.

- 정적 멤버 기반 접근 제어 모델
- 동적 멤버 기반 접근 제어 모델

4.1.1 클래스, 속성 기반 접근 제어 모델

객체지향 DBMS에서 정적 멤버 기반으로 DAC 정책을 적용한 초기의 접근 제어 모델은 Orion이며[12], 이는 DAC 정책을 지원하는 대부분의 객체지향형 접근 제어 모델들의 기초가 된다.

이 모델의 기본 구성은 관계형 DBMS에서 DAC 정책을 지원하는 접근 행렬 모델과 매우 유사하다. 단지, 접근 제어 모델에서 보호할 대상이 테이블과 뷰 대신에 객체지향 데이터베이스의 구조인 클래스와 속성이란 점이 차이가 있다.

Orion 접근 제어 모델의 중요한 특징은 묵시적 권한부여(implicit authorization) 개념이다. 묵시적 권한부여는 DBMS가 유지하는 접근 규칙 데이터베이스에서 주체, 객체, 그리고 접근 권리 각각의 함축 계층구조(implication hierarchy)들로 부터 새로운 접근 규칙을 유도하는 개념이다. 묵시적 접근 규칙이 존재하므로써 얻어지는 잇점은 DAC 정책을 지원하는 모든 접근 제어 모델에서 시스템 관리자 또는 사용자가 명시적으로 기술하는 접근 규칙의 갯수를 효과적으로 감소시켜, 접근 규칙 데이터베이스의 팽창을 방지할 수 있는 점이다.

Orion 접근 제어 모델이 관계형 DBMS를 위한 접근 제어 모델과 구분되는 또하나의 특징은 이 모델이 객체지향 DBMS의 구조적 특징인 계승, 복합 객체, 버젼 계층구조에 대한 접근 제어를 시행하는 것이다[12].

4.1.2 메소드 기반 접근 제어 기법

이는 객체지향 DBMS에서 대한 접근은 객체 인터페이스인 메소드를 통하여 모두 수행되기 때문에 사용자가 호출한 메소드에 대해 접근 제어를 시행하는 것이 효과적이라는 발상으로 부터 제안된 방법이다. 메소드를 기반으로 메소드 수행에 대해 접근 권리를 부여하는 대표적인 접근 제어 모델로 Iris, Data-hiding 접근 제어 모델 등이 있다[1, 3]

먼저, Iris 데이터 모델에서 속성과 메소드는 모두 함수로 표현되며, 속성은 저장 함수(stored function) 그리고 메소드는 유도 함수(derived function)로 정의된다. 따라서, 객체의 데이터는 함수의 집합으로 캡슐화되고, 객체 데이터를 접근하기 위해서는 적절한 함수를 사용자가 호출해야 한다. 따라서, 접근 제어를 위한 접근 규칙에는 각각의 사용자가 호출하도록 허용된 함수 집합을 기술한다.

새로운 유도 함수가 이미 존재하는 저장 함수 또는 유도 함수들로 부터 유도되기 때문에 이 유도 함수에 대한 접근 권한을 부여하는 방법은 다음과 같이 2가지가 있다.

- 동적(dynamic) 권한부여
  사용자가 유도 함수에 대해 동적으로 권한을 부여받는 경우, 이 사용자가 해당 유도 함수의 호출이 종료하기 위해서는 유도 함수의 기반이 되는 모든 함수들에 대해 호출 권리를 명시적으로 갖어야 한다.
- 정적(static) 권한부여
  사용자가 정적으로 권한을 부여받은 유도 함수를 호출하기 위해서는 유도 함수를 구성하는 함수들에 대해서 수행 권리를 기술한 명시적 접근 규칙을 갖지 않아도 된다.

반면에, Data-Hiding 모델에서는 Iris와는 달리 메소드의 형태를 공적(public) 메소드와 사적(private) 메소드로 구분한다. 한 객체에 정의된 사적 메소드는 오직 이 객체 또는 다른 객체에 정의된 다른 메소드에 의해서 호출될 수 있고, 반면에 공적 메소드는 객체의 소유자나 사용자가 직접 호출할 수 있는 메소드이다. 사적 메소드는 이를 호출하는 다른 메소드가 소속된 부분 즉, 동일 클래스에 같이 존재해야 하며, 이러한 사적 메소드를 호출할 수 있는 다른 메소드들의 집합을 호출 범위(invocation scope)라 한다. 따라서, 접근 제어는 사용자가 호출할 수 있는 공적 메소드를 중심으로 수행되며, 접근 규칙에도 공적 메소드에 대한 사용자 권리가 기술된다.

또한, 사용자가 실행시킨 특정 메소드가 수행하는 동안에 다른 메소드가 호출될 수 있으며,

이렇게 한 메소드가 수행 중에 다른 메소드를 호출하는 경우에도 접근 제어가 필요하다. 메소드 수행 과정에서 내부적으로 호출되는 메소드의 형태가 무엇이냐에 따라 접근 제어 처리 방법에 차이가 있으며, 이는 다음과 같은 원칙에 의해서 수행된다.

- 공적 메소드 호출
  내부적으로 호출되는 메소드가 공적 메소드 이면, 사용자는 호출되는 메소드에 대해서도 명시적인 수행 권리를 갖어야 한다.
- 사적 메소드 호출
  내부적으로 호출되는 메소드가 사용자에 의해서 수행된 공적 메소드의 호출 범위에 해당하면, 이 사용자는 내부 메소드를 수행할 수 있다.

4.2 객체지향 DBMS의 다단계 보안 모델

객체지향 DBMS에서 데이터의 다단계 보호를 시행하기 위해 객체지향 데이터베이스의 구조에 적합한 다단계 보안 모델로 SORION 모델, 메세지 필터(message filter) 모델, Millent-Lunt 모델 등이 있으며[10, 11, 14, 15], 본 절에서는 SORION과 메세지 필터 모델을 바탕으로 객체지향 DBMS에서의 다단계 보호 기술에 대해 설명한다.

4.2.1 SORION

이 모델은 ORION 데이터 모델을 기반으로 BLP 보안 모델을 기초로 하여 보안성 개념을 확장한 다단계 보안 모델이다[14]. 접근 제어를 위한 모델의 구성요소로는 주체, 객체, 접근 권리, 주체와 객체의 보안등급, 객체 보안등급의 제약조건, 그리고 사용자가 데이터에 접근할 때 사용자와 데이터 사이에서 정보의 흐름을 통제하여 올바른 정보의 분배가 이루어지도록 하는 보안 공리 등이 있다.

SORION 모델의 중요한 특징은 객체의 보안등급이 정보의 노출 가능성 배제와 올바른 정보의 접근을 보장하기 위한 6가지 형태의 제약조건에 의해 결정되도록 하는 것이다[15]. 이러한 제약조건은 객체지향 데이터베이스의 특징들인 객체, 클래스, 메소드, 단일 또는 다중 계승(multiple inheritance), 그리고 복합 객체 등에 대해서 각기 정의된다.

또한, 이러한 보안등급의 개념을 바탕으로 객체에 대한 사용자의 접근 제어는 아래에서 설명되는 6가지의 보안 공리들에 의거하여 이루어지며, 이는 데이터 사이의 정보의 흐름을 통제한다.

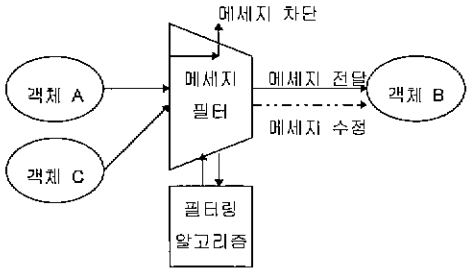
- 상향 판독 금지 원칙
  주체의 보안등급이 객체의 보안등급을 지배할 때, 주체가 객체에 대한 읽기 권리를 갖는다.
- 상향 기록과 하향 기록 금지 원칙
  주체의 보안등급이 객체의 보안등급과 동일한 경우에 이 객체에 대해 쓰기 권리를 갖는다.
- 메소드 수행 원칙
  이는 두가지 형태로 기술된다. 첫번째는 주체의 보안등급이 수행시킬 메소드의 보안등급과 이 메소드가 기술된 클래스의 보안등급을 지배할 때, 주체가 메소드에 대해 수행 권리를 갖는다. 두번째는 메소드가 수행되는 수준은 이를 호출한 주체의 보안등급 수준이 되어야 한다.
- 연쇄 메소드 수행 원칙
  하나의 메소드가 수행 도중에 다른 메소드를 호출하면, 호출한 메소드의 수행 보안등급이 호출되는 메소드의 보안등급과 이 메소드를 기술한 클래스의 보안등급을 지배하는 경우에만 호출된 메소드가 수행된다.
- 객체 생성 원칙
  하나의 메소드 수행 결과로 새로운 객체가

생성되면, 이 객체의 보안등급은 메소드를 수행시킨 주체의 보안등급과 동일하다.

4.2.2 메세지 필터 모델

메세지 필터 모델[10]은 SORION 다단계 보안 모델과는 달리 객체지향 시스템의 기본적 개념인 캡슐화 기능을 완전하게 활용하여 데이터에 대한 사용자의 접근을 통제하는 다단계 보안 모델이다.

객체지향 시스템에서 객체들 사이에서 정보를 교환하는 유일한 수단은 메세지이며, 이러한 메세지를 객체가 주고 받음으로써 객체들 간의 정보 흐름이 발생하기 때문에 메세지 필터 모델은 객체들 사이에서 상호 교환되는 메세지들을 (그림 5)와 같이 필터링하여 정보의 흐름을 통제한다.



(그림 5) 메시지 필터 모델

이 모델에서는 객체지향 데이터 모델에서 정의한 객체를 보안 모델의 주체와 객체로 고려하기 때문에 데이터베이스에 존재하는 객체는 BLP 모델의 주체와 객체가 될 수 있는 두 가지의 특성을 모두 갖는다. 객체의 보안등급은 객체가 생성되는 시점에 할당되며, 객체에 할당되는 보안등급은 SORION과 비슷하게 2가지의 보안 공리에 의해 제약된다.

그리고 메세지 필터 모델에서 모든 메세지는 하나의 객체에서 다른 객체로 직접 전달하는 것을 허용하지 않는다. 따라서, 메세지 필터는 객체들 사이의 교환되는 모든 메세지를 중간에서 가로채고, 메세지 송신 객체와 수신 객체의 보안등급을 기반으로 메세지의 처리 방법을 결정한다. 필터에서 메세지의 처리 형태는 메세지 전달, 메세지 차단, 제약된 메세지의 전달이 있으며, 이는 전달되는 메세지의 형태와 보안등급을 고려한 필터링 알고리즘에 의해서 하나의 종류로 결정된다.

5. 결론 및 향후 연구방향

본 고에서는 컴퓨터 보안 기술과 관련한 데이터베이스의 보안성, 무결성 그리고 이용성을 보장하는 기본적인 보안 서비스인 데이터베이스 시스템을 위한 여러 형태의 접근 제어 기술에 대한 내용을 개략적으로 살펴보았다. 현재 초고속정보통신망을 근간으로 데이터베이스 응용들이 분산되어 운영되고 있는 환경을 고려할 때, 데이터베이스 시스템이 보다 안전한 서비스를 제공하기 위해서는 기본적으로 사용자에 대한 인증 서비스가 완벽하게 제공되어야 하고, 이를 바탕으로 데이터베이스의 보안 유지 수단인 접근 제어 기술, 추론 방지 기술, 그리고 침입 탐지 기술 등이 통합된 서비스로 제공되어야 할 필요성을 인식할 수 있다.

최근의 데이터베이스 시스템의 보호를 위한 연구 동향은 분산(distributed) 데이터베이스 환경에서 정당한 사용자에게 보다 빠르고 정확하게 정보를 제공하는 동시에 정보의 간접적인 획득 수단인 추론을 방지하는 기술을 중심으로 연구하고 있다. 향후에는 이러한 연구와 더불어서 관계형 데이터베이스 시스템과 객체지향 데이터베이스 시스템이 상호 결합된 객체 관계형 데이터베이스(object relational database) 시스템에서 보안성 지원 기술의 연구가 수행되어야 할 것이다.

참고문헌

[1] Ahad R. et al, Supporting access control in an object-oriented database language, Proc of 3rd Conference on Extending Database Technology (EDBT), Vol 580, 1992.

[2] Bell D. E., La Padula L. J., Secure computer systems: mathematical foundations and model, Technical Report M74-244, MITRE Corp., 1974.

[3] Bertino E., Data hiding and security in an object-oriented database system, Proc of 8th IEEE Int. Conference on Data Engineering, 1992.

[4] Bertino E. et al, Authorizations in relational database management systems, Proc. 1st ACM Conference on Computer and Communication Security, 1993.

[5] Biba K. J. Integrity considerations for secure computer systems, Technical Report 76-372, MITRE Corp., 1977.

[6] Denning D. E., Cryptography and Data Security, Addison-Wesley, 1982.

[7] Denning D. E., Schlorer J., Inference controls for statistical databases, IEEE Computer, Vol. 16, No 2, 1983.

[8] Denning D. E. et al, The Sea View security model, Proc of IEEE Symp. On Security and Privacy, 1988.

[9] Griffiths P. G., Wade B., An authorization mechanism for a relational database system, ACM Trans. Database Systems, Vol.1, No 3, 1976.

[10] Jajodia S., Kogan B., Integrating an object-oriented data model with multilevel security, Proc of IEEE Symp. On Security and Privacy, 1990.

[11] Millen J. K., Lunt T. F., Security for object-oriented database systems, Proc. of IEEE Symp. On Security and Privacy, 1992.

[12] Rabitti F. et al, A model of authorization for next-generation database systems, ACM Trans. Database Systems, Vol.16, No.1, 1991.

[13] Silvano C. et al, Database Security, Addison-Wesley, 1995.

[14] Thuraisingham M. B., A multilevel secure object-oriented data model, Proc. of 12th National Computer Security, 1989.

[15] Thuraisingham M. B., Mandatory security in object-oriented database system, Proc. of Conference on Object-Oriented Programming: Systems, Languages, and Applications(OOPSLA), 1989.

주 광 로

1983년 전남대학교 계산통계학과 졸업 (이학사)
1985년 전남대학교 대학원 전산통계학과 졸업(이학석사)
1995년 전남대학교 대학원 전산통계학과 박사과정 수료

1985-현재 서강전문대학 전산과 부교수
관심분야 객체지향 데이터베이스, 정보통신, 정보보안

박 우 근

1983년 전남대학교 계산통계학과 졸업 (이학사)
1985년 전남대학교 대학원 전산통계학과 졸업(이학석사)
1994년 전남대학교 대학원 전산통계학과 박사과정 수료

1986년-현재 광주대학교 전산학과 부교수
관심분야 : 객체지향 데이터베이스, 퍼지 데이터베이스, 데이터베이스 보안, 데이터 마이닝