通信情報保護學會誌
第4卷 第1號, 1994. 3

이질형 분산 데이타베이스 시스템에서의 보안

강 석 훈*, 문 송 천**

1. 개 요

이질형 분산 데이타베이스 시스템은 기존에 서로 다른 목적을 위해 독자적으로 개발된 지역 데이타베이스 시스템을 통합해 새로운 분산 데이타베이스 시스템을 구축하는 방법으로 전역 데이타에 대한 서비스들을 제공한다. 이러한 서비스들을 제공하기 위한 설계 철학에는 지역 데이타베이스 시스템의 자치성을 보장하고, 서로 다른 기능에 대한 이질성을 은폐시켜야 한다.

데이타베이스의 자치성의 보장이란 지역 데이타베이스 시스템 관리자에게 스키마 구조, 전역 데이타베이스 구축에 관계된 지역 자료의 투시성과 갱신가능여부, 트랜잭션 동기화 정책의 선택, 그리고 이질형 분산 데이타베이스의 참가나 탈퇴에 대한 결정권을 부여하는 것을 의미한다.

이질성의 은폐를 위해 이질형 분산 데이타베이스는 상이한 스키마 설계에 기초를 둔 서로 다른 데이타 모델을 가지고 호환성 없는 소프트웨어가 운용되는 응용의 경우처럼 서로 완전히 다른 지역 데이타베이스들을 전역적으로 통합할 수 있도록 은폐성을 제공해야 한다. 따라서, 이질형 분산 데이타베이스 시스템을 개방형 시스템이라고 분류한다면 동질형 분산 데이타베이스 시스템은 상대적으로 폐쇄형 시스템이라고 할 수 있다. 또한, 이질성은 각 지역 사이트에 일정하지 않은 이름이 부여 되었을때도 발생한다. 예를 들어, 같은 의미를 갖는 여러 속성들의 사이트에 각각 다른 이름이 부여 될 수 있고, 또는 더욱 나쁘게는 서로 호환이 안되는 속성을 가진 다른 사이트에 같은 이름이 사용될 수도 있다.

강제적인 보안 정책과 임의적인 보안 정책이 통합 운영되어야 할 강결합된 이질형 분산 데이타베이스 시스템의 보안 요구사항과 연산은 새로운 연구분야로서 해결해야 할 문제들이 산적해 있다. 이질형 분산 데이타베이스의 목적은 사용자로 하여금 여러개의 하부 요소를 구성하는 데이타베이스들의 자료에 접근, 병합 및 갱신을 실행할 수 있게 하는데 있으므로 자료 접근에 대한 액세스 제어는 이질형 분산 데이타베이스의 전역 보안 정책뿐만 아니라 참가하는 사이트의 지역 보안 정책의 결합도 강약에 크게 의존한다. 보안기법은 전역 보안 연합에 가입하거나 탈퇴하는 개별 사이트의 자치성과 각 사이트의 자료공개 정책의 변경 여부에 영향을 받게 된다. 또한 하부 요소 데이타베이스들의 이질성에 의해서 이질형 데이타베이스 시스템에서의 보안 기법은 더욱 복잡해진다. 사이트에 따라 서로 다른 보안 정책들을 하나로 통합하는 것은 매우 어렵고 일관성을 유지하기도 힘들다. 사용자의 인증에 따른 다수의 서로 다른 데이타베이스들로부터 통합 유지되는 자료의 액세스 제어에 대한 문제들과 해결방안이 본 고의 주요 내용이다.

* 정회원, 한국과학기술원 정보 및 통신공학과
** 정회원, 한국과학기술원 정보 및 통신공학과

1.1 다단계 보안 및 일단계 보안을 위한 액세스 제어

액세스 제어를 위한 보안 정책은 임의적 액세스 제어(discretionary access control: DAC) 정책과 강제적 액세스 제어(mandatory access control: MAC) 정책으로 크게 구분할 수 있다[Lunt89]. DAC 정책은 주체나 주체가 속해있는 그룹들의 식별자를 근거로 객체에 대한 액세스를 제한하는 방법이며, MAC 정책은 객체에 포함된 정보의 비밀등급(sensitivity)과 주체에 부여된 등급별 비밀 취급 인가(clearance)를 기반으로 하여 객체에 대한 액세스를 제어하는 방법이다. MAC정책은 비밀 등급별 보안(multilevel security: MLS)기법 구현을 위한 방법론의 핵심이 된다.

대부분의 상용 데이타베이스 관리 시스템들이 채택하고 있는 보안 유지 방법은 데이타에 대한 사용자들의 사용 권한을 제어하는 임의적 액세스 제어 방식들이다. 임의적 액세스 제어 방식이라고 명명된 이유는 데이타에 대한 사용 권한을 사용자 임의대로 다른 사용자들에게 넘겨줄 수 있는 액세스 제어 방식이기 때문이다. 이러한 DAC방식은 대부분의 정직한 내부 사용자들에 대한 정보의 누출을 방지하는 경우에는 적합할 수 있으나, 악의적인 침입자들의 트로이목마를 이용한 데이타의 액세스 또는 컴퓨터 바이러스에 의한 데이타의 액세스는 반드시 제한되고 방지되어야 함에도 불구하고 원천적으로 방지할 수 없는 결함을 가지고 있다. 트로이목마는 프로그램 내에 인가되지 않은 사용자에게 정보를 누출시키는 악의의 코드를 수록한 것이다. 예를 들어, 유틸리티 프로그램 중의 정렬 프로그램에 트로이목마가 감춰져 있다면, 사용자가 정렬 프로그램을 불러 자신의 화일들을 정렬시키고자 할 경우마다 인가받지 못한 사용자에게 자신의 화일들을 통채로 복사시킬 수가 있는 것이다.

따라서, DAC 방식의 결점을 극복하기 위한 강제적인 액세스 제어 방식이 개발되었다. MAC 방식은 주체와 객체라는 용어에 의해 기술된 Bell-LaPadula모델에 기초한다[Lunt 90]. 객체는 데이타 화일, 레코드 또는 레코드 내의 필드로 이해될 수 있으며, 주체는 객체들에 대한 액세스를 요청할 수 있는 활성화된 프로세스이다. 모든 객체는 비밀등급이 할당되며, 각각의 주체도 등급별 비밀취급 인가가 되어야 한다. 비밀등급은 아래에 기술한 두개의 구성 요소들로 이루어진다.

첫째, 계층적 등급으로서 통상 1급 비밀(top secret), 2급 비밀(seret), 3급 비밀(confidential), 그리고 비밀 해당상항 없음(unclassified)들로 구분된다.

둘째, 취급 분야 집합으로서 예를 들면 국방, 행정, 외교 분야등을 들수 있다.

Bell-LaPadula모델은 데이타 액세스를 할 경우, 아래의 제약조건을 부가한다.

(1) 단순 특성(Simple Security Property, 상향 열람 금지): 주체의 비밀등급이 객체의 비밀등급보다 동일하거나 높을 경우에만 객체의 읽기 액세스가 허용된다.

(2) 복합 특성(*-Property, 하향 기록 금지): 주체의 비밀등급이 객체의 비밀등급보다 동일하거나 낮을 경우에만 객체에 대한 기록 액세스가 허용된다.

위에서 기술한 두개의 제약조건들은 상위 비밀취급 인가자로부터 하위 비밀 취급 인가자에게로의 정보 누출이 없도록 고안된 것이다. 이러한 제약조건들은 강제적이고 시스템에 의해 모든 읽기와 기록 연산에 대해 자동적으로 실행되기 때문에 트로이목마에 의한 침투를 점검하고 방지할 수 있다. 그러나 최근에 밝혀진 바로는 Bell-LaPadula의 제약 조건들을 항상 올바르게 실행할지라도 보안 상의 문제가 발생할 수 있음이 판명되었다[Koga 90]. 안전한 시스템은 데이타에 대한 직접적인 비밀 누출 뿐만 아니라 간접적인 비밀 누출을 통한 불법적인 정보의 흐름을 차단할 수 있어야 한다. 비밀채널(covert channel)이 후자에 속하는 간접적인 비밀 누출의 형태이다. 비밀채널은 상위 비밀 취급 인가자가 하위 비밀 취급 인가자에게 정보의 양에 관한 다소를 불문하고 간접적인 정보 누출 수단을 제공할 수 있다.

MLS-DBMS측면에서 언급해야 할 또다른 관점이 있다. 미 국방성의 요구사항[DoD 83]을 만족하기 위해서는 시스템이 안전하다는 것을 반드시 증명할 수 있어야 한다. 이러한 목적으로 정보 보호용 DBMS 설계자들은 TCB(trusted computing base, 보안커널 또는 참조 모니터)개념을 준수하여 설계한다. TCB는 시스템 내의 모든 보안 관련 행위들에 대해 책임이 있어서 데이타베이스에 대한 모든 액세스들이 우회 통과될 수 없도록 하고 적절한 조치를 취한다. TCB는 보안 규격을 올바르게 실행하고 있음을 증명할 수 있도록 간단 명료하게 설계되어야 하며, 외부침투가 불가능한 안전함이 증명될 수 있도록 TCB 이외의 다른 시스템 구성 요소들과 격리 되어야 한다.

미 국방성의 TCSEC에는 각종 컴퓨터 시스템의 보안 기준을 평가할 수 있는 평가기준 행렬표가 기술되어 있다. A1, B3, B2, B1, C2, C1, 그리고 D와 같은 등급이 부여되며, 각 등급별로 시스템이 해당 등급에서 반드시 보유해야하는 요구사항들을 기술하고 있다. 간단히 요약하면, C1과 C2등급의 시스템은 데이타에 대한 DAC기법을 제공해야 하며, B1등급의 시스템은 MAC기법을 제공해야 한다. B2 또는 B3, A1와 같은 상위 등급의 시스템은 특히 비밀채널에 대한 보다 향상된 보증이 제공되어야 한다. A1등급에서는 가장 엄격한 정보보호 기준이 제시된다. D등급은 A,B 또는 C등급들로 평가될 필요가 없는 보안 요구가 필요하지 않은 모든 시스템들로 구성된다.

본고는 다음과 같이 구성되어 있다. 2절은 이질형 분산 데이타베이스를 위한 보안 체계의 골격을 설명한다. 특히 이 골격이 어떻게 보안을 지원하는가에 중점을 두게 된다. 또한 이질형 분산 데이타베이스 보안의 미해결 연구분야들과 이미 제기된 문제들로 다루게 된다. 3절과 4절은 강제적 액세스 제어를 지원하는 다단계 보안과 일단계 보안의 임의적 액세스 제어에 대한 문제를 다루게 된다.

2. 이질형 분산 데이타베이스 시스템의 보안 체계

이질형 분산 데이타베이스의 다섯 단계 스키마 구조[Shet 90]는 지역 데이타베이스를 위한 기본적인 세 개의 스키마가 포함되어 있다: (1) 외부 스키마들의 모음 또는 사용자 뷰, (2) 개념적 스키마, 그리고 (3) 물리적 스키마. 여기에다가 이질형 분산 데이타베이스가 사용하게 되는 이질성의 은폐와 하부구성 데이타베이스들의 자치성을 위한 두개의 스키마가 더 필요하다. 이것들은 개념적 스키마를 출력 스키마, 구성 스키마, 그리고 이질형 분산 개념 스키마들로 대치한 것으로 이해할 수 있다. 그림 1에서 제시된 스키마 단계들은 필요한 사상이나 자료 전송을 제공한다.

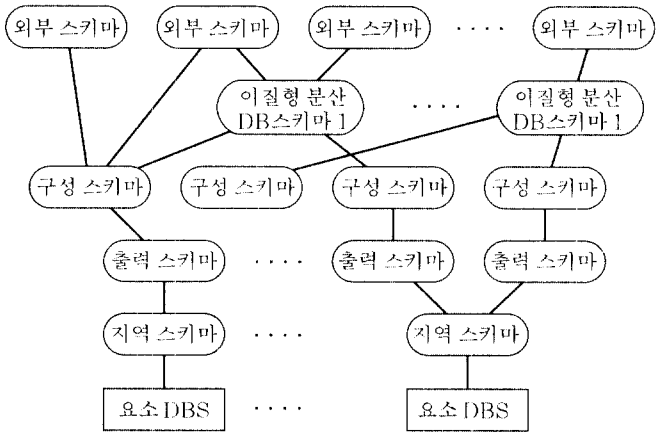

그림 1 이질형 분산 데이타베이스 시스템의 스키마 구조

출력 스키마는 지역 데이타베이스의 스키마위에서 사상을 제공한다. 사상은 각 사이트에서 이질형 분산 데이타베이스로 보여질 수 있는 자료를 제한한다. 하나의 사이트는 사실 한개 이상의 이질형 분산 데이타베이스에 참가할 수 있으며, 그림 1에서처럼 각각의 이질형 분산 데이타베이스에 대해서 서로 다른 출력 스키마와 보안 정책을 가질 수도 있다.

구성스키마는 각 사이트의 데이타베이스를 위한 이질형 분산 데이타베이스의 공통 표현을 제공한다. 지역 데이타베이스의 출력 스키마에서 이질형 분산 데이타베이스의 전역 자료 모델로 변환시켜 전송한다. 예를 들어, 하나의 사이트는 객체 지향적이며, 다른 사이트는 네트워크 스키마를 가지고 있고, 이질형 분산 데이타베이스 상호교환 언어는 관계형이라고 하면, 구성 스키마들은 각 사이트에서 관계형 표현으로 전송해야 한다.

이질형 분산 데이타베이스 스키마는 자료 접근 가능성의 일정한 표현을 이루는 구성 스키마들의 조합으로서 이질형 분산 데이타베이스의 개념 스키마이다. 이질형 분산 데이타베이스 스키마는 자료에 대한 사용가능 여부와 위치 정보에 대한 디렉토리를 제공한다. 실제 자료의 통합도는 사이트별로 다를 수 있다.

다섯 단계 스키마 구조에서는 구성 스키마위에 출력 스키마가 위치한다. 즉, 출력 스키마는 구성 스키마가 기술하는 것을 이질형 분산 데이타베이스 상호교환 언어의 형태로 보여주어야 함을 의미한다. 액세스 제어를 통한 보안기능 강화를 위해 출력 스키마를 지역 스키마 위에, 구성 스키마 밑에 위치토록 한다.

2.1 이질형 분산 데이타베이스 구조에서의 보안

보안 정책과 구현된 매카니즘은 사이트별로 서로 다를 수 있으므로 부가적인 보안 게이트웨이들과 제어들이 사용되어야 한다. 이질형 분산 데이타베이스의 보안은 분산방식을 적용할 수도 있고 중앙 집중식으로 제어할 수도 있으며, 두가지 방식이 혼합적용될 수도 있다.

사이트의 자치성과 설계의 단순화를 위해 각 사이트는 자신의 변경사항을 최소화시키도록 해야 한다. 어떤 자료가 이질형 분산 데이타베이스에 출력되는가에 대한 제어는 지역 사이트의 결정에 달려 있으므로, 그림 1에서처럼 출력 스키마는 지역 스키마 바로 위에 놓이게 된다. 그리고, 구성 스키마는 이질형 분산 데이타베이스 상호교환 언어에 달려 있으므로 구성 스키마는 출력 스키마위에 위치시킨다. 그 이유는 전역 액세스 제어를 통한 보안기능 강화를 위해 기본적인 다섯 단계 구조로 부터 변경된 것이다.

이러한 변경된 구조에서 지역 사이트는 자기 자신의 지역 스키마와 출력 스키마를 자신의 제어하에 두게된다. 이것은 그림 2의 아랫부분에 나타나 있다. 사이트에 있는 지역 사용자들은 자신의 지역 데이타베이스와 직접 상호작용을 유지하게 된다. 이러한 방식으로 이질형 분산 데이타베이스는 구성 스키마와 이질형 분산 데이타베이스 스키마의 통합과 이질형 분산 데이타베이스 사용자들을 위한 외부 뷰들의 생성에 대한 사상들의 제어를 분리하여 유지할 수 있게 된다. 이것은 그림 2의 윗부분에 나타나 있다.

그림 2는 지역 사이트에 기반을 둔 액세스 제어들과 이질형 분산 데이타베이스의 전역적 액세스 제어들간의 경계를 나타내고 있다. 그림 2는 윗쪽의 두개의 상자로 경계표시한 것처럼, 서로 분리된 제어를 가진 두개의 부 이질형 분산 데이타베이스를 보여주고 있다. 이질형 분산 데이타베이스 1(왼쪽)은 검색의 효율과 시스템의 신뢰를 향상시키기 위해 자료를 복사하여 사본을 관리하게 된다. 사본 관리는 그 자료를 가지고 있는 하부 요소 사이트의 동의를 얻어서 이루어지게 된다.

이질형 분산 데이타베이스 액세스 제어를 구현한 시스템들과 소프트웨어들은 물리적으로 개개의 사이트들과 분리시키거나 인증된 사이트에 부분적 또는 전체적으로 완전 중복시키게 된다. 그림 2에

서 사이트 제어를 나타내는 상자와 이질형 분산 데이터베이스 제어를 나타내는 상자가 겹치는 부분(그림 2의 왼쪽)이 바로 부분적으로 위치시키는 것을 나타낸다. 오른쪽에 있는 사이트는 두개의 다른 출력 스키마들을 구현하였다. 왼쪽에 있는 사이트에서는 두개의 이질형 분산 데이터베이스로 똑같은 자료를 출력하는 것에 비해 오른쪽에 있는 사이트에서는 각 이질형 분산 데이터베이스마다 별도의 출력 스키마를 둔다.

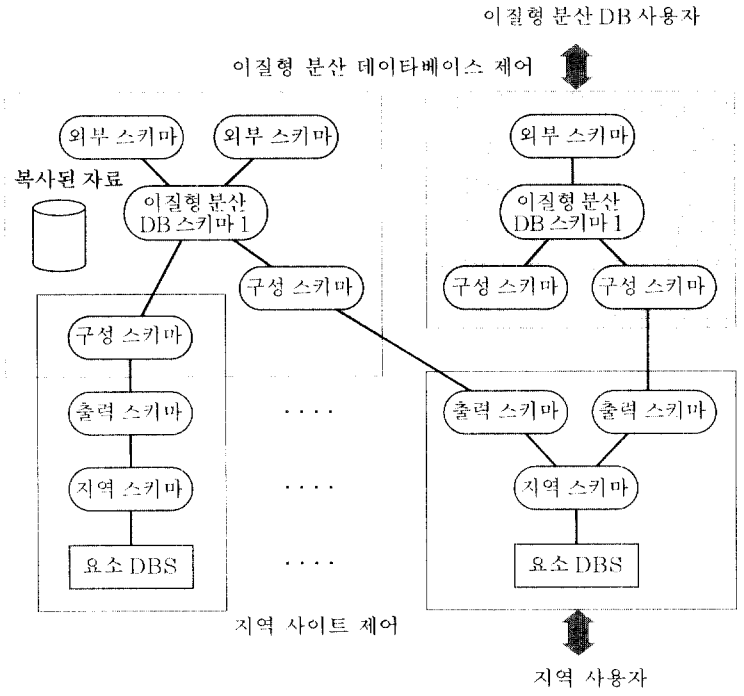

그림 2 보안을 고려한 이질형 분산 데이타베이스 시스템의 스키마 구조

2.2 이질형 분산 데이타베이스 시스템의 보안 구현을 위한 고려사항

이질형 분산 데이타베이스 구조에 따라 쉽게 해결할 수 없는 다양한 보안 문제들이 제기되며, 제시된 해결책들도 특정 응용을 위한 이질형 분산 데이타베이스의 목표마다 서로 다를 수 있다.

우리는 이제부터 이질형 분산 데이타베이스의 보안에 대한 단계적으로 접근할 것이다. 즉, 첫단계로 제한된 목표를 가지고, 단기간에 실현될 수 있는 보안체계를 다루게 될 것이다. 기능성과 보증의 단계를 높임으로써 결과적으로 설계와 구현에 더 많은 시간이 드는 다음 상위 단계의 좀더 복잡한 목표로 진전이 가능하다. 이것이 시스템 설계의 새로운 개념은 아니지만 이질형 분산 데이타베이스 보안의 범주로서 관심을 갖는 요체이다. 예를 들어, 이질형 분산 데이타베이스에 신뢰할 수 있는 전역적 보안통신망이 필요할 경우 통신규약에 암호화 기법을 사용함으로써 통신보안을 달성할 수 있다. 통신 패턴으로부터 드러나는 비밀채널까지도 적절한 수준의 잡음 메시지들을 혼합시켜 상위등급의 통신보안을 유지할 수가 있다.

다른 사이트들로부터의 자료를 다루기에 지역 사이트들이 충분히 신뢰할 보안 수준이 안되는 경우에는 복수 사이트들의 요구를 처리할 수 있는 하나나 그 이상의 이질형 분산 데이타베이스 서버

노드들을 둘수 있다. 이 방법은 하부 요소 데이타베이스들에서의 보안 요구를 줄이고, 서버 노드에 참가하지 않는 이질형 분산데이타베이스 사이트들에 비해서 높은 보호도를 제공하게 된다. 이때 사용자들은 그들의 지역 사이트가 아니라 이질형 분산 데이타베이스 서버에 인증을 요구하게 된다. 물론 복수 사이트 요구들에 대한 전역적 보안 정책은 미리 설정 되어야 한다. 구현을 위한 최초 설계 단계는 복수사이트에서의 자료 추출 연산만을 허용하고 갱신 연산은 단일 사이트로 국한시키는 방안을 선택한다. 사이트 자치성의 보장 정도와 임의의 사이트에서 복수의 사이트에 대한 갱신을 허용할 것인지에 관한 절충문제는 다음 설계 단계의 고려사항이다.

다음 설계 단계에서는 지역 사이트들의 보안에 대한 신뢰도를 높이기 위해 정교한 검증기법이 필요할 수도 있고, 이질형 분산 데이타베이스 사용자에게 부가적인 기능성을 제안할 수도 있을 것이다. 이질형 분산 데이타베이스 시스템을 위한 액세스 제어의 보안 처리 능력에 대한 단계적 개발 전략은 단기간의 구현을 위한 기본적인 방법론이 되며 좀더 복잡한 문제 해결을 위한 경험적 연구 기반을 제공할 수 있는 것이다.

3. 이질형 분산 데이타베이스 시스템들을 위한 다단계 보안

지난 10년간 주로 관계형 자료 모델에 근거한 다단계 보안 데이타베이스 관리 시스템들이 개발되어 다단계 보안 데이타베이스들 시제품중 일부는 상용화 되었다. 이러한 데이타베이스 시스템들에서 여러 비밀 등급에 있는 사용자들은 기밀 취급 인가범위에 따라 미세한 단위로 구성된 다단계 보안 데이타베이스에 접근하고 공유할 수 있게 된다. 다단계 보안 데이타베이스 시스템들이 많아질수록 보안상의 문제없이 이들을 서로 연결하여 다단계 보안 환경을 지원하는 이질형 분산 데이타베이스를 구축하는 것이 반드시 필요해질 것이다. 실제로 동작하는 시스템을 제작하기 위해서는 미리 해결해야 할 연구과제들이 산적해 있다. 그 이유는 (1)다단계 보안 이질형 분산 데이타베이스 시스템 개발의 첫걸음에 불과한 다단계 동질형 보안 분산 데이타베이스 시스템의 개발이 최근에 와서야 시작되었고, (2)단지 일단계 보안 이질형 분산 데이타베이스 시스템이라 할지라도 개발되기 위해서는 먼저 풀어야 할 문제들이 여전히 남아 있기 때문이다.

비록 다단계 보안 이질형 분산 데이타베이스 시스템의 개발에 대한 완전한 해답을 구할려면 한 세대나 남았지만, 적어도 현재 이미 개발된 이질형 분산 데이타베이스 시스템과 데이타베이스 보안기술들을 사용해서 개발상의 문제들을 실험해 볼 수는 있다. 본 절은 이질형 분산 데이타베이스 관리 시스템들을 위한 필수 보안 요건들 중 자료 분산, 이질성 은폐, 그리고 자치성 보장에 대한 문제들에 대해 논의할 것이다.

3.1 자료 분산

다단계 보안 이질형 분산 데이타베이스 시스템에 저장된 자료는 서로 다른 보안 등급이 배정되게 된다. 이제 이질형 분산 데이타베이스인 전역 시스템과 지역 데이타베이스 시스템 사이에 관계형 모델로 가정한 분산 환경에서 절편화와 사본의 문제에 관해서 논의하고자 한다.

가. 절편화

다단계 보안 관계형 데이타베이스는 다단계 보안 관계들의 집합으로 이루어져 있다. 다단계 보안 관계란 각 튜플에 보안 등급이 부여되어 있는 관계를 의미한다. 다단계 보안 환경에서는 서로 다른 보안 등급에 있는 사용자들이 같은 객체에 대해서 서로 다른 뷰를 제공할 수 있어야 한다. 이러한 매카니즘을 다중치 배정(polyinstantiation)[Thur 90]이라고 부르며, 동일한 주 키를 갖는 두개의 서로 다른 튜플이 서로 다른 보안 등급으로 존재할 수

있도록 허용하는 것이다[Jajo 90].

재결합은 특정한 보안 등급에서 다단계 보안 관계의 뷰를 만드는 과정이다. 보안 등급 L에서 재결합 연산은 등급 L로 한정되어 있는 관계의 모든 튜플들을 포함하게 된다. 이것은 사용자의 비밀 취급 인가등급 이하로 분류된 모든 튜플들을 읽을 수 있기 때문이다. 다중치 배정이 제공되는 환경에서 사용자는 자신의 등급보다 낮은 다중치 배정을 그의 뷰에서 제거하도록 요청할 수 있다. 이렇게 한다면, 재결합이 수행되고 있는 보안 등급중에서 가장 높은 등급의 튜플들만 보여지게 된다.

다단계 보안 데이타베이스는 분할되어 서로 다른 사이트들에 저장될 수 있다. 절편화는 수평적, 수직적, 또는 복합된 형태로 이루어 질수 있다. 튜플들이 여러 사이트들에 걸쳐서 다중치 배정이 될 수도 있다. 즉, 같은 주 키를 가지지만 보안 등급이 다른 두개의 튜플이 서로 다른 위치에 존재할 수 있다는 것이다. 이렇게 절편들이 서로 다른 사이트들에 저장될때 등급 L에서의 재결합 과정은 먼저 지역 사이트에서 등급 L의 관계 뷰를 형성한 다음 각 지역 뷰들을 전역 뷰를 만들기 위해 결합하면 된다.

나. 사본 유지

자료는 효용성과 효율적인 검색을 위해 다수의 장소에 사본을 유지할 수 있다. 다단계 보안 환경에서 자료는 보안상의 이유로도 복사되어 질 수 있다. 예를 들어, 다단계 보안 환경에서는 모든 구성요소들이 동일한 보안 등급으로 다루어 질수 없다. 어떤 구성요소는 비밀로 분류되지 않은 자료부터 이급 비밀까지 다룰 수 있고, 또 다른 구성요소는 일급 비밀 등급까지 다룰 수 있다고 하자. 자료 복사에 의한 사본 유지가 이루어지지 않는다면, 두번째 구성요소에 로그인한 일급 비밀 취급 인가 사용자가 첫번째 구성요소에 있는 비밀 자료가 아닌 것과 삼급 비밀 및 이급 비밀 자료에 접근할 수 있는 유일한 방법은 일급 비밀 취급 인가 사용자의 질의가 첫번째 구성요소로 경로 전달시키는 것이다. 보안의 관점에서, 그 질의가 믿을 수 있는 경로를 통하지 않는다면 결코 처리를 허용해서는 안될 것이다. 이렇게 한다고 할지라도, 비밀 채널들이 존재할 가능성은 항상 있다. 비밀채널을 제거하는 방법중에 하나는 첫번째 요소 DBS에 있는 자료를 두번째 요소 DBS에 복사해두는 것이다. 두번째 요소 DBS는 일급 비밀만 다루기 때문에 복사된 자료들은 모두 일급 비밀 등급으로 분류된다. 그러나, 이질형 분산 데이타베이스의 관점에서 본다면 이러한 복사는 바람직하지 않다. 왜냐하면 첫번째 요소 DBS에 있는 데이타베이스 관리자나 시스템 보안 요원이 자신이 속한 지역 데이타베이스에 대해 전적으로 제어권을 행사하지 못하기 때문이다. 다시 말하면, 보안과 자치성 사이에는 타협점을 찾기 위한 절충이 있어야 한다.

3.2 이질성

보안이 보장된 이질형 분산 데이타베이스 시스템에서도 여러가지 종류의 이질성의 은폐가 필요하다. 어떤 형식의 이질성은 일단계 보안 환경에서 나타날 수도 있고 다른 형식의 이질성은 다단계 보안때문에 생긴다. 이 절에서는 이질적인 요소 DBS들간의 접속 연결에 관련된 원초적인 문제들과 보안상의 영향에 대해 논의하게 될 것이다.

가. 스키마 또는 자료 모델의 이질성

서로 다른 구조를 가진 데이타베이스들이 모두 동일한 자료 모델로 표현된 것은 아니므로 서로 다른 개념적 스키마들이 하나로 통합되어야 한다. 이렇게 하기 위해서는 임의의 자료 모델의 구조를 다른 자료 모델의 구조로 번역해 주는 번역기가 있어야 한다. 다단계 보안 환경에서는 각각의 자료 모델들이 그 자신안에 다단계 보안 구조를 가지고 있어야 한다는 것을 뜻한다. 그러므로, 어떤 다단계 보안 자료 모델 구조는 다른 다단계 보안 자료 모델의 구조로 변환될 경우 번역과정에서 사용자가 하나의 자료 모델에 대해서 어떤 특정한

객체에 접근할 수 없었다면 동일한 객체에 대해 다른 자료 모델로 접근하는 경우에도 허용불가의 원칙이 지켜져야 한다. 스키마의 이질성을 다루기 위해서 객체 지향 접근 방식이 유용할 수 있다. 이 방법은 사용자들로 하여금 전체 시스템에 대한 공통 뷰를 가지게 한다는 것이다. 그러면 번역기는 공통적인 표현에서 개별적인 표현으로 구조를 변경해주어야 한다. 물론 이 반대의 일도 해주어야 한다.

나. 트랜잭션 관리 기법의 이질성

서로 다른 데이타베이스 관리 시스템들은 트랜잭션 처리를 위해서 서로 다른 동시성 제어 알고리즘을 사용할 것이다. 이에 따라 로킹, 타임스탬핑, 확인 메카니즘들을 통합시키는 트랜잭션 관리 기법이 개발되고 있다[Bern 87]. 이질형 다단계 보안 데이타베이스 관리 시스템에서 보안문제까지 연관시킨다면 문제는 더욱더 풀기 어려워 진다. 표준의 동시성 제어 알고리즘은 보안에 취약성이 있다. 예를 들어, 이단계 로킹 기법은 높은 비밀등급의 프로세서에서 낮은 비밀등급의 프로세서로 지연시간 정보를 이용하여 비밀채널을 개설할 수 있음이 증명되었다[Tsai 90]. 이질형 트랜잭션 관리 환경에 맞도록 수정된 동시성 제어 알고리즘의 통합은 아직도 연구를 해야할 미해결 과제이다.

다. 질의 처리의 이질성

서로 다른 데이타베이스 관리 시스템들은 서로 다른 질의 처리와 최적화 전략들을 가지고 있다. 연구자들은 분산된 질의 최적화를 위한 전역 질의 처리 비용 모델을 개발하고 있다. 다단계 보안 환경에서 개별적인 질의 처리 비용 모델들은 보안 정책, 사용되는 저장 메카니즘, 분류된 자료의 양에 의존하며, 전역 질의 처리 비용 모델은 전역 보안 정책에 의거하여 설계된다.

라. 질의어의 이질성

서로 다른 데이타베이스 관리 시스템들은 각기 다른 질의어들을 사용할 것이다. 데이타베이스 관리 시스템들이 모두 관계형 모델에 기초하고 있다고 하더라도 어느 하나는 SQL과 다른 관계형 대수를 사용할 수 있다. 일정한 인터페이스 언어를 개발하기 위해 표준화 노력들에 보안이 미치는 영향도 연구되어야 할 것이다. 예를 들어, 보안 구조들에 적합한 SQL의 확장이 필요하게 될 것이며 이러한 확장들은 사용자에게 일정한 인터페이스를 제공하기 위해서 통합되어야 한다.

마. 제약조건의 이질성

서로 다른 데이타베이스 관리 시스템들은 서로 다른 무결성 조건을 적용하게 된다. 예를 들어 어떤 데이타베이스 관리 시스템은 모든 직원이 주당 적어도 40시간 이상을 일해야 한다는 조건을 가질 수 있는 반면 또 다른 데이타베이스 관리 시스템은 그러한 조건을 강요하지 않을 수도 있다. 보안이 요구되는 환경에서는 임의적 보안 제약 조건이나 강제적 보안 제약 조건같은 부가적인 제약 조건이 필요하다. 서로 다른 요소들에 대한 제약 조건들은 서로 혼란을 가져올 수 있다. 이러한 차이점들은 전역적으로 통합 조정되어야 한다.

바. 의미적 이질성

자료는 서로 다른 요소들에 의하여 서로 다르게 해석될 수 있다. 예를 들어, 한 요소 DBS에서는 어떤 객체의 주소를 국가 이름으로만 인식하지만 다른 요소 DBS는 그 객체의 주소를 우편 번호, 거리 이름, 시 이름, 국가 이름으로 인식할 수도 있다. 사실 의미적 이질성은 다루기가 매우 힘들다고 인식되어 있다. 다단계 보안 환경에서는 이 문제가 더욱 어려워진다. 예를 들어, 한 요소 DBS의 보안 명칭은 다른 요소 DBS에서는 전혀 다른 뜻이 될 수 있기 때문이다. 이러한 불일치를 해결하기 위해서는 표준화 노력이 필요하다.

사. 보안 정책의 이질성

지역 데이타베이스 관리 시스템들은 임의적 보안 뿐만 아니라 강제적 보안에도 각기 다른 보안 정책을 사용하게 된다. 이외에도 서로 다른 인증과 무결성 메카니즘들을 사용하게 된다. 예를 들

어, 어떤 시스템은 자기의 비밀 등급 이하로만 읽기가 허용되고 쓰기는 자기의 등급에서만 가능한 다단계 보안 정책을 적용한다고 하자. 반면에, 다른 시스템에서는 자기의 비밀 등급 이하로 읽기가 허용되고, 쓰기는 자기 등급 이상이 가능할 수도 있다. 더군다나, 지역 데이타베이스 관리자나 시스템 보안 요원은 전역 보안 정책보다 더욱 제한적인 보안 정책을 표방할 수도 있다. 전역 보안 정책을 수립하고 시행하기 위해서는 각기 다른 정책들이 통합되어 불일치들이 해소되어야 한다.

아. 동일한 객체에 대한 보안 등급의 다른 분류

한 객체는 어떤 노드에서 이급비밀로 분류되고, 그 다음 노드에서는 일급비밀로 분류될 수 있다. 이러한 보안 등급부여 및 분류상의 차이점들은 전역적으로 통합 조정되어야 한다.

3.3 자치성

이질형 분산 데이타베이스 시스템의 요소들인 지역 데이타베이스 시스템은 보안 정도에 따른 자치성을 가질 수 있다. 각 요소들의 데이타베이스 관리자나 시스템 보안 요원은 그들이 통제하는 자료에 누가 접근 가능한지를 결정한다. 요소 DBS의 자치성에는 통신 자치성, 수행 자치성, 결합 자치성, 설계 자치성등이 있다. 각각의 종류에 대해서 논의하면 다음과 같다.

가. 통신 자치성

통신 자치성의 완전 보장은 요소 DBS가 자기가 통신하고 싶은 상대를 결정할 수 있도록 한다. 다단계 보안 환경에서는 명칭들이 다르게 해석되지 않는 한 일급 비밀만을 다루도록 된 기계가 이급 비밀에서 비기밀까지를 다루는 기계에게 자료를 보내지 못하게 하는 것과 같은 추가적인 제한이 있다.

나. 실행 자치성

실행 자치성이란 어떤 방법으로든 이질형 분산 데이타베이스의 사용자들에 의해서 요소 DBS들의 지역 연산 실행들이 영향받지 않음을 보장한다. 이것은 다단계 보안 환경에서는 문제를 일으킨다. 예를 들어, 이질형 분산 데이타베이스의 비기밀 사용자가 특정한 요소 DBS의 트랜잭션의 수행을 지시한다고 하자. 만약 이미 그 요소 DBS에서 수행되기를 기다리는 이급 비밀의 지역 트랜잭션이 있다고 하면 실행 자치성은 비기밀의 트랜잭션은 기다려야 한다고 결정할 것이다. 즉, 상위 등급의 사용자의 행동들이 하위 등급에 영향을 미치는 것이다. 이것은 비밀채널을 유발할 가능성을 충분히 내포하고 있음을 의미한다.

다. 결합 자치성

결합 자치성의 완전 보장은 요소 DBS가 다른 요소 DBS들과 언제 무슨 자료를 공유할 것인가를 결정할 수 있도록 한다. 이질형 분산 데이타베이스 환경의 경우에는 요소 DBS가 언제, 어떤 연합에 참여할 것인가, 탈퇴할 것인가도 결정하게 된다. 사본 유지를 위한 자료 복사는 결합 자치성과 충돌을 일으킨다. 예를 들어, 요소 DBS 1에 의해서 관리되는 자료가 요소 DBS 2에 복사된다고 하고, 요소 DBS 1이 연합을 탈퇴한다고 하자. 그러면, 요소 DBS 2에 남아있는 그 자료는 같이 제거되어야 한다. 그러나 보안을 이유로 하위등급 자료를 보다 상위등급으로 복사해야 할 필요가 있다. 바로 이것이 결합 자치성을 제한하다. 그러므로 결합 자치성은 바람직한 특성임에도 완전한 결합 자치성이 가능한 지는 아직 의문의 여지가 남아있다.

라. 설계 자치성

설계 자치성의 완전보장은 각 요소 DBS가 자기 자신의 설계를 선택할 수 있도록 한다. 예를 들어, 구성요소는 (1)관리할 다단계 보안 등급자료, (2)적용되는 보안정책, (3)질의어 처리 및 사용되는 트랜잭션 관리 알고리즘, (4)자료와 명칭들의 의미적 번역들을 결정할 수 있다. 이질형 분산 데이타베이스 시스템의 보안 기법을 개발하는데 있어서 어려움 중의 하나는 서로 다른 보안 정책들

을 통합하는데 있다. 서로 다른 정책들은 설계 자치성 때문에 존재한다.

여기서 논의된 다양한 문제들에 덧붙여서, 보안 환경의 주요한 관심들 중에 하나는 공인이다. 만약에 요소 DBS들이 자치성을 가지고 있다면, 각각의 지명된 승인 기구들은 자기자신의 시스템을 인증할 자유가 있다. 그러나 시스템 전체를 인증하기 위해서는 각기 다른 지역 데이타베이스 시스템의 승인 기구들과 전체 연합인 이질형 분산 데이타베이스 시스템의 승인 기구간에 타협이 있어야 한다. 따라서 이에 대한 인증 자치성이 새로 도입될 필요가 있을 수 있다.

4. 이질형 분산 데이타베이스 시스템을 위한 일단계 보안

이질형 분산 데이타베이스 시스템에서의 임의적 액세스 제어는 전체 연합의 일부인 복수의 지역 데이타베이스 시스템들의 자료에 대한 제어와 배치를 필요로 한다. 만약에 그 지역 시스템들이 이질적이라면, 이런 경우가 보통이지만, 임의적 액세스 제어의 적용은 힘들다. 왜냐하면 다양한 지역 데이타베이스 시스템들이 임의적 액세스 제어 정책들을 적용하고 나타내는데 있어서 서로 다르고 호환되지 않는 메카니즘을 사용하기 때문이다. 특히, 연합에 소속된 복수의 사이트들로부터의 자료를 포함하는 질의들은 복수이고 이질적인 지역 데이타베이스 시스템들의 액세스 제어 메카니즘들에 의해 처리되기 때문이다. 전역 시스템들의 사용자들에게 일정한 액세스 제어 가능을 제공할 수 있는, 지역 시스템들의 액세스 제어 메카니즘들을 배치하는 것은 어려운 일이다.

더욱더 어려운 문제는 지역 시스템들이 자치적으로 동작할 수 있도록 해주는 이질형 분산 데이타베이스가 갖추어야 할 필요사양에 의해 발생한다. 이것은 각 지역 데이타베이스 시스템이 자기가 관리하는 자료에 지역 시스템 또는 전역 시스템의 사용자가 접근할때 자신에 의해 저장되고 결정되는 자료의 제어를 관리한다는 말이다. 아래에 보여질 내용처럼, 보안 뷰들과 같은 임의적 액세스 제어를 적용한 통상적인 방법은 지역 시스템의 자치성을 위한 요구사항을 갖춘 이질형 분산 데이타베이스 시스템의 경우에서는 깨어지기 시작한다.

4.1 가정

다양한 상업용 데이타베이스 시스템들이 운영되고 서로 약결합된 통신망을 가진 컴퓨터들이 주어지고, 각 지역 시스템의 자치성을 보장하면서, 이러한 데이타베이스들을 합쳐서 이질형 분산 데이타베이스를 구축하고자 한다. 또한 이질형 분산 데이타베이스 시스템에 임의적 접근 제어를 적용한다고 가정하자. 이러한 문제를 해결하기 위해 전역 데이타 모델을 가진 개별 시스템들을 통합시키는 접근 방법이 사용될 것이다.

문제를 보다 정확히 정의하기 위해서 몇가지 가정이 필요하다. 첫째, 지역 데이타베이스 시스템들은 서로 다른 자료 모델을 가지고 있다고 가정한다. 이럴 경우 서로의 코드는 교환될 수 없으며 각자는 서로 독립적인 액세스 제어를 적용할 수 있게 된다. 둘째, 이질형 분산 데이타베이스 시스템은 사용자에 대한 보안 인증을 할 수 있으며, 시스템들간의 보안 통신을 보장하고, 복수의 지역 데이타베이스 시스템들의 자료를 포함하는 전역 질의를 지원한다고 하자.

4.2 이질형 분산 데이타베이스 시스템에서의 액세스 제어

지역 데이타베이스 시스템은 각자 자신만의 독립적인 액세스 제어 시스템을 가지고 있다. 이는 자치성에 대한 가정 때문이다. 또한 이질형 분산 데이타베이스 시스템은 복수의 지역 시스템으로부터의 자료를 다룰 액세스 규칙들을 위한 그 자신만의 액세스 제어 시스템을 가져야 한다. 또한 전역 시스템은 어떠한 지역 시스템도 할 수 없는(왜

냐하면, 그들은 전체 연합의 일부이므로) 의미 종속적인 액세스 규칙을 적용할 수 있는 그 자신만의 액세스 제어시스템을 사용해야 한다.

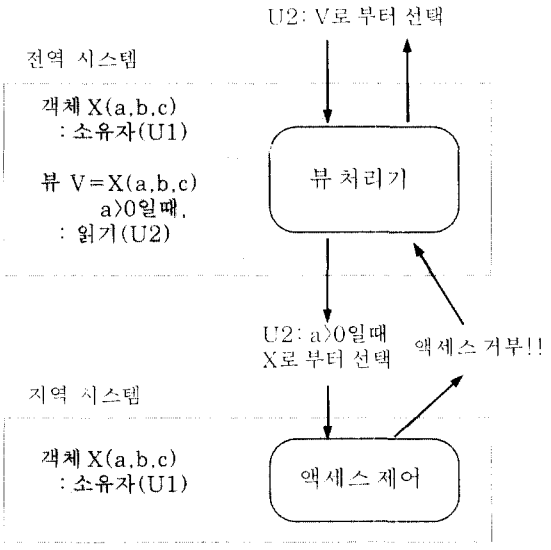

그림 3 표준 뷰 처리 알고리즘에 의한 전역적 액세스 제어

이러한 문제들이 발생할 수 있음을 보이기 위해 뷰의 정의에 의해 질의내의 뷰에 대한 참조를 대신할 수 있는 표준 뷰 처리 알고리즘을 사용하여 임의적 액세스 제어들을 적용하는 보안 뷰를 사용하는 이질형 분산 데이타베이스를 가정하자. 그림 3에 이러한 내용을 도시하였다. 사용자 U1은 지역 시스템에 있는 객체 X를 소유하고 있다. 이질형 분산 데이타베이스 시스템은 각 지역 시스템의 자료 모델들을 통합하여 전역적인 자료 모델을 만들기 때문에, X는 이질형 분산 데이타베이스 시스템의 전역 모델에도 존재하며, U1에 의해서 소유된다. 이질형 분산 데이타베이스 시스템의 전역 모델내에서 U1은 X에 대한 뷰 V를 생성한다고 가정하고, 다른 사용자 U2가 V에 접근한다고 하자. 그러면 U2는 직접 X에 접근할 권한이 없게 된다.

이제 U2가 뷰 V를 통해 이질형 분산 데이타베이스 시스템에 자료를 요구하는 질의를 입력했다고 가정한다. 이질형 분산 데이타베이스 시스템의 뷰 처리 기술을 이용하여 X의 견지에서 V의 정의에 의해 이 질의내의 참조를 뷰 V로 바꾸어 놓는다. 이 수정된 질의는 처리될 X를 위한 자료를 포함하고 있는 지역 시스템으로 넘겨지게 된다. 지역 시스템내의 액세스 제어 시스템은 사용자 U2가 X에 액세스하는 것을 허용하는 액세스 규칙이 없으므로 이 질의를 거부하게 된다. 지역 시스템이 전역 시스템의 뷰 V와 같은 의미 종속적인 접근 규칙을 규칙을 규정하는 어떤 방법을 가지지 않는 한, U1은 U2가 지역 시스템의 뷰 V를 처리하는데 필요한 자료에 접근하게 허용할 수가 없다. 지역 시스템은 의미 독립적인 정책만을 지원하도록 가정했음을 상기하라. 그러므로, U1이 지역 시스템에서 할 수 있는 최선의 방법은 U2에게 X에 접근할 수 있도록 하는 것이다. 그러나 이것은 U2가 전체 연합을 통하지 않고 단지 지역시스템만을 이용해서 X의 모든 것에 접근하도록 허용하는 바람직하지 않은 방법이므로 해결책이 될 수 없다.

위 결과들에서 나타난 문제는 두가지 가정에서 비롯되었다. 첫째, 모든 지역 시스템이 의미 종속적인 액세스 규칙들을 가질 수 없다고 가정했다. 대부분의 관계형 데이타베이스 시스템들은 이러한 규칙을 가질 수 있지만, 다른 종류의 데이타베이스나 파일 시스템들은 그럴 수 없을 수도 있다. 뷰나 다른 메카니즘(이 메카니즘은 액세스 규칙들의 표현력에는 미치지 못한다고 가정한다.)을 사용하여 모든 지역 시스템들이 의미 종속적인 액세스 규칙들을 가진다고 할지라도 비슷한 문제들이 발생할 여지가 있다. 둘째, 각 사이트는 그 자신의 자치성을 유지하며 그 결과로 전역 시스템에 의해 내려진 액세스 결과들을 신뢰하지 못한다고 가정했다. 어떠한 응용프로그램에서는 전역 시스템에서의 지역 데이타베이스 시스템들에 대한 자치성을 요구하지 않을 수도 있으나 언젠가는 자치성이 요구되는 경우가 있을 것이며 위에 보여진 것처럼 액세스 제어를 적용하는데 있어서 문제를 발생시킬 것이다.

5. 결 론

이질형 분산 데이타베이스 시스템은(Heterogeneous Distributed Database System: HDDBS) 지역 데이타베이스 관리 시스템에 의해 자치적으로 관리되는 지역 데이타베이스 시스템(DBS) 사이에 상호 연산을 지원하는 시스템이다. 지역 데이타베이스 시스템은 전역 스키마가 없는 약한 결합을 형성하거나 연합 DBS를 형성하는 강한 결합을 이룬다. HDDBS 시스템에서 데이타베이스 보안은 매우 주요한 기능이나 구현에 있어 아래에 기술한 이유들로 대단히 복잡하고 어려운 일로 예측된다.

첫째, HDDBS는 지역 데이타베이스 시스템보다 훨씬 많은 사용자 그룹이 있고 이들 다수의 사용자에 대해 보다 정밀한 액세스 제어가 필요하다.

둘째, 지역 데이타베이스 시스템은 각기 다른 사용자들의 그룹에 의해 저장된 데이타의 상이한 부분만을 공유하려는 것이 통상적인 경우이다.

셋째, HDDBS에서 지역 데이타베이스 시스템을 동시에 액세스가 가능하여 권한 없는 사용자에 의한 정보 유출의 위험이 단일 DBS에 비해 매우 크다.

넷째, 지역 데이타베이스 시스템들은 서로 다른 DBMS에 의해 자치적으로 운용되며, 각기 다른 MAC 및 DAC 기법들이 사용될 수 있다.

대부분 관계형 DBMS는 현재 액세스 제어와 뷰 기능으로 보안 기능을 지원한다. 사용자는 SQL의 GRANT 문장을 사용하여 릴레이션을 생성, 변환, 수정 그리고 선택하는 권한을 부여 받는다. 사용자는 또한 부여된 권한을 다른 사용자에게 전파하는 특권을 보유할 수 있다. 이 특권은 시스템 보안 책임자가 REVOKE 문장을 사용함으로써 취소될 수 있다. 관계형 DB 시스템에서 뷰 기능은 시스템 관리자 또는 보안 책임자에게 융통성을 부여하여, 기저 릴레이션으로부터 유도된 어떠한 릴레이션도 될 수 있는 뷰에 대한 권한을 허용할 수 있다. 다단계 보안 등급을 갖는 MLS-DBMS는 다양한 보안 등급으로 분류된 데이타를 저장하고, 사용자의 비밀취급 변경이 가능하면서도 비밀취급 인가가 되지 않은 사용자들로 하여금 비밀 데이타가 유출되는 것을 방지 할 수 있어야 한다. 이러한 보안 기법은 보다 융통성이 있고; 보호의 단위는 튜플 또는 속성의 단위까지 세분화될 수 있다. 비록 HDDBS와 같이 TCB를 요구하는 진정한 의미의 다단계 보안 시스템과 같은 방대한 소프트웨어 시스템을 만드는 것은 대단히 어려운 작업임에는 틀림없으나 결코 불가능한 것은 아니다. MAC기법의 개념은 HDDBS에서도 적용될 수 있다[Kang 92].

국내 연구동향 중 현재 한국과학기술원 문송천 교수 실험실에서 진행 중인 확장 연구과제로서 국내 최초 연구 개발된 관계형 데이타베이스 시스템인 IM의 차기 버전인 상용 IM에 보안기능을 구현시키는 연구활동이 1994년 중반기에 완료될 예정이며, 역시 KAIST에서 제작된 분산 데이타베이스 관리체계인 DIME(Distributed Information Management)에 다단계 보안기능을 설계 및 구현하는 연구가 1994년 말에 완료될 예정이다.

참 고 문 헌

[Bern 87] P.A. Bernstein, V.Hadzilacos, and N. Goodman, "Concurrency Control and Recovery in Dat-abas Systems," Addison-Wesley, Reading, MA, 1987.

[DOD 83] "Department of Defense Trusted Computer System Evaluation Criteria," Depart-ment of Defense, National Computer Security Center, 1983.

[Jajo 90] S.Jajodia and R.Sandhu, "Polyinstantiation Integrity in Multilevel Relations," Proc. IEEE Symp. on Research in Security and Privacy, May 1990,pp. 104-115.

[Kang 92] Sukhoon Kang and Songchun Moon, "An Integrated Access Control in Heterogeneous Distributed Database Systems," Journal of Microprocessing and Microprogramming, 1992, forthcoming.

[Koga 90] B. Kogan and S. Jajodia, "Concurrency Control in Multilevelsecure Databases Using Replicated Architecture, "Proc. ACM SIGMOD Int'l. Conf. on Management of Data, May 1990.pp.153-162.

[Lunt 89] T.F.Lunt, "Access Control Policies for Database Systems," In C.E. Landwehr, Editor, Database Security Ⅱ: Status and Prospects, North Holland, 1989.

[Lunt 90] T.F.Lunt, D.E.Denning, R.R. Schell, M.Heckman, and W.R. Schockley, "The SeaView Security Model,"IEEE Trans. on Software Engineering, Vol. 16, No. 6, Jun. 1990, pp. 593-607.

[Shet 90] A.Sheth and J.Larson, "Federated Database Systems for Managing Distributed, Heterogeneous, and Autonomous Databases," ACM Computing Surveys, Vol.22, No.3, pp. 183-236, Sep. 1990.

[Thur 90] B. Thuraisingham and P.D. Stachour, "Design of LDV: A Multilevel Secure Relational Database Management Sys-tems," IEEE Trans. on Knowledge and Data Engineering, Vol. 2, No.2, Jun. 1990, pp. 190-209.

[Tsai 90] W.T.Tsai and T.F.Keefe, "Multiversion Concurrency Control for Multilevel Secure Database Systems," Proc. IEEE Symp. on Research in Security and Privacy, May 1990.pp. 369-383.

□ 著者紹介

강 석 훈

한양대학교 전자공학과 학사
한국과학기술원 전산학과 석사
현재 한국과학기술원 정보 및 통신공학과 박사과정
금성정밀(주) 기술연구소 선임연구원

문 송 천

1971년 3월 - 1975년 1월 숭실대학교 전자계산학과 학사
1975년 3월 - 1977년 2월 한국과학원 전산학과 석사
1981년 8월 - 1985년 1월 미국 일리노이 대학교(어바나 샴페인) 전산학 박사
현재 한국과학기술원 정보 및 통신공학과 부교수
유럽정보과학회 (EUROMICRO)이사