通信情報保護學會論文誌
第5卷 第1號, 1995. 3

객체의 분할과 통합에 의한 스키마 기반 데이타베이스 보안 모델

강 석 준*, 김 용 원**, 황 종 선***

A Secure Database Model based on Schema using Partition and Integration of Objects

Seog-Jun Kang*, Yoeng-Won Kim**, Chong-Sun Hwang***

요 약

분산 환경을 고려한 보안 데이타베이스 모델에 효율적인 접근 제어와 자료가 가지는 가치의 중요도에 따라 정보의 흐름을 제어하기 위한 다단계 기법을 도입하는 연구들이 진행되어 왔다. 기존의 기법들은 문제점을 내포한 상태에서 연구가 이루어졌다. 문제점은 첫째, 다단계로 보호되는 전역적인 자료에 대한 관리가 거의 불가능하다는 점이다. 둘째, 부분과 전역의 자료에 대한 과도한 접근 취소로 실제 사용자의 접근 허용여부와 접근을 원하는 자료의 상관 관계를 분리하기가 어려워 진다. 기존의 기법이 가진 문제점으로 인해 성능의 하락과 사용에 있어 유연성을 제공할 수 없다.

본 논문에서는 분산 환경에서 자료에 대한 보호를 쉽게 얻을 수 있고 전역적인 자료의 효율적인 관리와 사용자가 접근하고자 하는 자료에 대한 접근 취소가 일어나지 않는 스키마를 이용한 다단계 보안 데이타베이스 모델을 제안했다.

Abstract

In distributed environments, the DB secure models have been being studied to include the multi-level mechanism which is effective to control access according to the level of the data value. These mechanisms have the problems. The first, it is impossible to maintain the global data which is protected in the multi-level mechanism. The second, the access and the relation of the data is not clear due to the access revocation between the local data and the global's.

In this paper, we proposed the mechanism using shema. The mechanism doesn't have the access revocation, and provides the protection of the data and the control to the global data.

* 고려대학교 전산과학과 대학원
** 건양대학교 정보관리학과
*** 고려대학교 전산과학과 교수

1. 서 론

자료가 각 지역에 분산 및 중복되어 있는 환경에서 컴퓨터 내의 자료를 보호해야 하는 것은 매우 중요한 과제이다. 자료 공유의 용이성과 시스템 관리자 및 사용자에게 시스템 구축 및 사용에 유연성을 제공하여야 하며 보호를 위해 사용자 인증과 자료에 대한 보호기법이 필요하다.

자료의 보호는 물리적 접근제어를 통해서 이루어질 수 있으며 물리적 접근제어는 중앙 집중 시스템에서와 같이 사용자가 소수일 경우 쉽게 얻을 수 있다. 그러나 분산환경과 같이 다수의 사용자와 방대한 자료에 대해서 효과적인 물리적 접근제어와 사용자 인증은 실제로 불가능하다. 컴퓨터 통신의 급격한 확산에 따라 컴퓨터 자원이 분산된 환경에서 물리적 접근제어만으로는 컴퓨터 내의 자료를 보호한다는 것은 자원의 보호를 보장할 수 없으며 자료의 효용성을 떨어뜨리는 문제점을 수반하고 있다.

자료를 보호하기 위한 기존의 기법[1]은 자료의 흐름을 제어하는 기법, 추론을 방지하기 위한 기법과 자료객체에 대한 암호화를 통해 정보에 대한 직접적인 접근을 통제하는 기법 등이 이용되고 있다. 속 모델, 접근행렬 모델, 정보 흐름 모델 등이 대표적이며 사용자의 권한을 검사하는 것을 근간으로 하여 제시된 모델들이다.

자료의 흐름을 제어하는 기법으로서 속모델은 정보를 일정한 수준으로 분할된 저장장소에 분리해서 기록한다[11]. 접근하고자 하는 자원에 대한 사용자 권한 검사와 자료객체를 저장 위치가 다른 디스크로 분리한다. 속모델은 다단계 보호 개념이 추가되지 않은 보호 모델로서 시스템 관리자나 상황에 따라 객체에 대한 분할이 이루어지는 점이 다른 다단계 모델과 다른 점이다.

접근 행렬 모델에서는 행으로 접근 주체를 표현하고 종으로 객체를 표현하여 사용자가 접근할 수 있는 자료를 행렬의 형태로 표현한 모델로서 이것은 희소 행렬의 형태를 갖으므로 희소 행렬을 연결 리스트 형태로 표현한 ACL(Access Control List)를 사용한다.

정보 흐름 모델은 정보가 상위의 자료객체가 하위의 주체나 객체에 복사나 이동이 일어나지 못하도록 그 흐름을 제한하는 모델이다. 정보 흐름 모델에서 정보의 복사나 흐름을 제어하기 위해 보안정책의 필요성이 제시되었으며 이는 시스템의 특성상 큰 비중을 차지한다.

발전된 형태의 다단계 보안 모델에서는 위에서 기술된 모델과 데이타베이스라는 특수성을 이용한 기법들이 제안되었다. 자료에 대한 접근 가능 여부를 판단해서 암호화된 형태로 보여주는 기법등 다양하나 이는 기본적으로 사용자 권한과 사용자 능력을 기반으로 하여 접근을 제한하는 기법[3]과 연산의 종류를 제한하는 기법이다. 분산환경으로 이러한 기법들을 확장할 때 바람직하지 못한 결과를 낳는다. 사용자마다 고려해야 할 많은 자료객체, 사용자 권한을 고려할 때 많은 전송 부하와 접근 취소가 발생하고, 전역과 지역간에 등급의 일관성을 유지하기가 힘든 문제가 있다.

보안 등급으로 인한 정보에 대한 접근제한으로 발생하는 접근 취소로 실제 통신망의 사용율이 하락된다[10]. 다단계 시스템에서 갖는 이러한 문제점은 정보의 공유 측면에서 생각할 때 효율적이지 못하다.

정보의 공유에 효과적이면서도 자료를 효율적으로 관리하는 이상적인 보안 기법은 사용자에게 투명하며 짧은 처리시간과 시스템 사용에 있어 유연성을 제공하여야 한다. 기존의 기법을 분산환경에 적용할 때는 통신 환경만을 고려하였으므로 자료의 암호화가 중복되는 양상을 갖게 되어 성능 하락이 불가피하였다. 암호화의 중복으로 인한 성능 하락으로 자료객체의 암호화보다는 정보의 하부 접근 단계에서 자료에 대한 접근 허용 여부를 통해 효과적인 자료에 대한 보호를 얻을 수 있는 기법[10]이 필요하다.

본 논문에서는 분산환경에서 자료를 효율적으로 관리하고 정보 공유에 유리한 분산 데이타베이스 시스템에서 자료 보호와 자료 보안등급의 일관성을

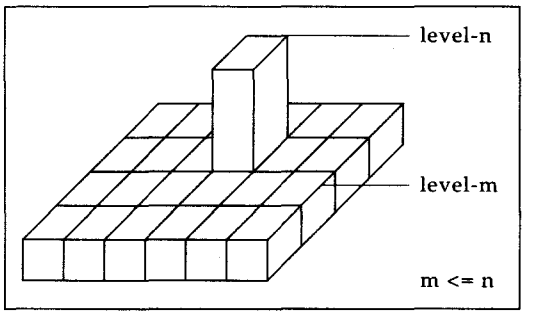
용이하게 유지할 수 있는 스키마를 활용한 자료객체에 대한 보호를 통해 정보의 접근 단계에서 미리 접근 허용 여부를 결정하는 기법을 제안한다.

2. 데이타베이스 시스템 내의 자료 보호 기법의 고찰

기존의 중앙 집중 데이타베이스 시스템에서는 접근 단위로 나뉘어진 자료를 암호화와 접근제어를 통해 보호하고 있다. 자료객체가 가진 가치의 중요성을 고려한 다단계 보안 모델에서는 자료 객체에 주어진 등급을 유지하고, 접근을 제어하는 것에 초점을 맞추고 있다. 다단계 보안 모델에서는 등급이 상이하게 할당된 자료객체를 보호하기 위해 저장된 물리적 레코드 전체 혹은 레코드 필드에 대한 접근을 제어하고 있다. 접근을 제어하는 단위가 각 레코드마다 상이하게 나타나므로 접근취소가 발생하게 되고 이런 접근 제어 기법은 사용자에게 투명하지 않다. 과도한 접근 취소는 상대적으로 많은 통신 부하를 갖게하므로 분산환경에 적합하지 않다.

2.1 Seaview 모델

사용자 뷰에 대한 조작을 가한 Seaview 모델에서는 스키마가 일정하게 유지되면서 접근하고자 하는 자료가 사용자의 등급에 따라 변환된 형태를 갖게 된다. 시스템의 관점에서는 하나의 암호화된 형태와 암호화되지 않은 평문의 두가지 형태로 보여지게 된다. Seaview 모델의 변환과정을 〔그림 1〕과 같이 표현할 수 있다. Seaview 모델에서 사용한 polyinstantiation 기법[4]은 하나의 객체에 대해서 여러 개의 상을 갖게 하는 기법으로써 자료객체에 대한 보호를 위해 사용자의 등급과 자료객체의 등급의 비교에 따라 자료객체의 변환 과정이 주축이 된다.



〔그림 1〕 Seaview 모델의 변환 과정

Seaview 모델의 변환과정은 사용자는 스키마를 통해 자료의 존재를 알 수는 있으나 자료가 가지는 실제 내용을 추론하는 것이 불가능하다는데 기법의 초점이 맞추어져 있다. Seaview 모델은 실제로 암호화가 이루어질 때 변환의 과정이 가장 핵심인 기법이나 변환 과정에서 생기는 문제점을 해결하기에는 기법 자체에 문제점을 안고 있다.

Seaview 모델의 자료가 〔표 1〕과 같이 구성되어 있다 가정할 때 문제점은 다음과 같다.

〔표 1〕 저장된 자료의 형태

Project				
no	Dept.	manager	budget	due_dat
1	KOREA Univ.	Prof. Hwang	100,000 $	94. 12. 12
2	YONSEI Univ.	Prof. Moon	50,000 $	95. 3. 5
3	HANYANG Univ.	Prof. Byun	40,000 $	94. 11. 15
⋮				

접근하고자 하는 자료가 〔표 2〕와 같을 때 보호 또는 변환이 필요한 자료가 속성 "manager"의 실제값 "Prof. Hwang"이라 할 때 자료객체가 가지는 의미를 계속 유지하면서 변환할 수 있는 기법은 실현 불가능하다. 변환 기법을 실현하기 위해서 전역에서 나타나는 자료객체 각각에 대한 정보와 이를 변환하기 위한 기법이 필요하며 이것은 개발자로 하여금 데이타베이스 전체에 대한 자료 입력 값을 고려해야 한다는 부하를 갖게 한다.

〔표 2〕 접근하고자 하는 자료

1	KOREA Univ.	Prof. Hwang	100,000 $	94. 12. 12

2.2 CDT 모델

CDT(Cluster Definition Table) 모델[5]에서는 저장될 자료의 형태에 대해 범위값과 나타날 자료의 값을 미리 분류하여 저장될 클러스터의 형태가 미리 정해지고, 이의 형태에 따라 클러스터의 등급이 정해지게 된다. 사용자의 등급과 접근하고자 하는 클러스터와의 비교를 통해서 그에 대한 접근을 제한하는 기법을 사용하고 있다. 클러스터의 형태는 〔표 3〕과 같은 형태로 표현되며 이는 사용자나 데이타베이스 시스템의 관점이 아니고 상대적으로 하부 저장구조인 자료객체의 관점에서 이루어진다.

〔표 3〕 자료의 저장형태

ID	Desc-Id Set	Record-Id
C1	{D12, D21, D31, D41}	R1, R2, R3, R4
C2	{D13, D21, D31, D41}	R7, R8, R9
C3	{D12, D22, D31, D41}	R11, R15
C4	{D13, D21, D32, D42}	R21, R22, R23, R25
C5	{D13, D22, D32, D42}	R14

CDT 모델은 세가지 문제점을 가지고 있으며 다음과 같다. 첫째, 실제 스키마의 일부만 사용하는 경우 시스템에서 이를 처리하는 것은 계산 부하를 갖는 다는 것을 의미한다. 클러스터화된 레코드의 등급을 처리하는 경우 필요한 속성을 제외한 나머지 부분의 처리는 과도한 보호의 가능성을 안고 있다. 클러스터를 검색하고 사용자 뷰를 조작하는 것은 더 많은 시간과 연산이 필요하다. 단점의 원인은 제시한 기법에서 클러스터링 기법 자체에 내포되어 있다.

둘째, 학교내의 스키마를 가정해서 D1이 직업, D2가 수입, D3이 대학원 혹은 학부, D4가 나이라면 C1은 다음과 같은 조건을 만족해야 할 것이다.

```
C1 <== if ((D1 == student)
          and (D2 < 100000)
          and (D3 == under graduate)
              (D4 < 25))
```

CDT 모델에서 속성은 제한된 값만을 가질 수 있으며 개발자가 이런 제한된 값을 모두 고려하는 것은 불가능하며 실제 이런 고려가 이루어졌다 할지라도 스키마의 변경이나 등급을 따로 새롭게 구성해야 할 경우의 부하는 더욱 심각할 것이다

셋째, 숫자 개념의 속성인 경우 범위값을 쉽게 적용할 수 있으나 문자인 속성은 클러스터링을 사용한 등급의 부여시 속성이 가질 수 있는 값이 한정되는 결과를 갖게 된다. 사용자가 미리 정해진 자료 이외에 다른 자료를 삽입할 경우 이에 대한 등급의 부여는 정확하다는 확신이 없으므로 실제 저장되는 자료는 미리 정해진 자료(특히 문자 부분)만이 가능할 것이다. 저장되는 자료의 값이 정해진 데이타

베이스는 실제 사용에 효용이 없다 할 수 있다.

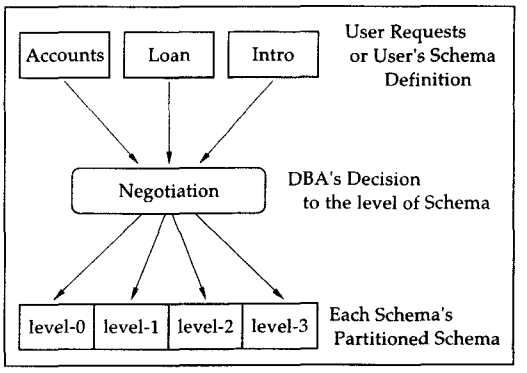
결과적으로 CDT 모델에서는 보호가 불필요한 부분에 대한 등급 할당에 따라 자료객체에 대한 과도한 접근 취소가 발생한다.

3. 스키마의 분할과 통합

스키마를 이용하여 자료객체에 대한 접근을 제한하는 기법은 접근단위가 스키마로 정의되고 정보의 등급도 스키마가 구성된 단위로 이루어지도록 하는 것이다. 스키마에 등급을 부여하기 위해 스키마 생성시에 속성이 갖는 자료 가치에 따라 스키마 분할이 이루어지도록 한다. 전역에 위치한 스키마에 등급을 부여하여 자료를 관리하는 것이다.

3.1 스키마의 등급 분류와 분할

스키마는 생성시 각 속성이 갖게 되는 자료의 가치에 따라 스키마의 분할이 이루어진다. 스키마 분할은 등급 부여의 전처리 단계로써 분할된 스키마는 데이타베이스 관리자들에 의해 등급이 결정된다. 지역 데이타베이스가 그 사용을 위해 전역 데이타베이스 시스템으로 제출될 때 등급을 표시하는 꼬리표가 부착된다. 그러나 스키마 등급의 결정은 그 타당성을 위해 데이타베이스 관리자들간의 협상에 의해서 이루어져야 한다.



〔그림 2〕 스키마 등급의 협상 과정

스키마에 대한 사용자의 요구나 정의 발생시 〔그림 2〕에서와 같이 전역 데이타베이스 관리자, 지역 데이타베이스 관리자들과 실제 사용자들 사이에 협상이 필요하다. 지역 데이타베이스 관리자들은 지역에서 필요한 스키마의 요구가 발생시 협상의 과정과 자료의 유지에 대한 관리를 책임지고 있다. 전역 데이타베이스 관리자는 실제로 각 스키마의 등급을 결정하는 책임과 스키마에 적절한 등급을 부여하여 효율을 높이기 위한 조율과정을 관리한다.

데이타베이스 사용자는 전역 데이타베이스 관리자가 등급을 정의한 스키마상에서 데이타 스키마 브라우저를 통해 사용자 뷰를 생성 및 조합하거나 관리자가 정의한 사용자 뷰를 사용한다.

3.2 스키마의 통합

스키마의 분할을 통해 스키마 단위로 이루어지는 등급의 분류는 이미 이루어져 있는 상태에서 사용자가 스키마를 직접 활용하기 위해서 등급 별로 통합이 필요하다.

스키마 통합을 이용하여 분산 데이타베이스에서 보안을 제공하기 위해서 지역과 전역간에 자료의 검색이 스키마 단위로 이루어지고, 전송되는 자료객체나 스키마에 꼬리표가 부가되는 기법이 사용된다.

label-based 기법은 스키마와 전송되는 객체에 대한 등급인 Classification의 표시와 사용자의 능력을 Clearance의 등급을 부가한 다단계 능력을 표시하기 위한 기법이다.

사용자의 등급이 결정된 후 사용자가 실행하는 명령은 시스템이 사용자에게 부가한 등급을 포함한 다단계 Capability-based 형태이다.

사용자의 모든 연산은 다단계로 등급이 붙여진 형태의 능력[7]을 갖으며, 이것은 사용자가 연산을 행할 때마다 시스템이 사용자의 등급과 객체의 등급을 비교하여 접근허용 여부를 판단하게 된다.

1. 스키마 생성시
(스키마의 통합을 위한 지역 스키마 관리자와 전역 스키마 관리자의 스키마 처리 과정)
   a. 지역 스키마 관리자
      새로 정의된 스키마를 등급을 부여하여 전역 스키마 관리자에게 제출
   b. 전역 스키마 관리자
      1) 제출된 스키마의 등급 검사 및 스키마 자료 갱신
      2) 사용자 요구시 스키마 검색 및 등급에 따라 스키마 통합

2. 스키마 삭제시
   a. 지역 스키마 관리자
      삭제될 스키마 정보를 전역 스키마 관리자에 제출
   b. 전역 스키마 관리자
      1) 삭제될 스키마 등급 검사
      2) 삭제될 스키마 검색
      3) 등급화된 스키마에서 스키마 삭제
      4) 삭제된 스키마 정보 각 지역 스키마 관리자에 전송

〔그림 3〕 스키마 통합과 삭제시 지역 및 전역 스키마 관리자 역할

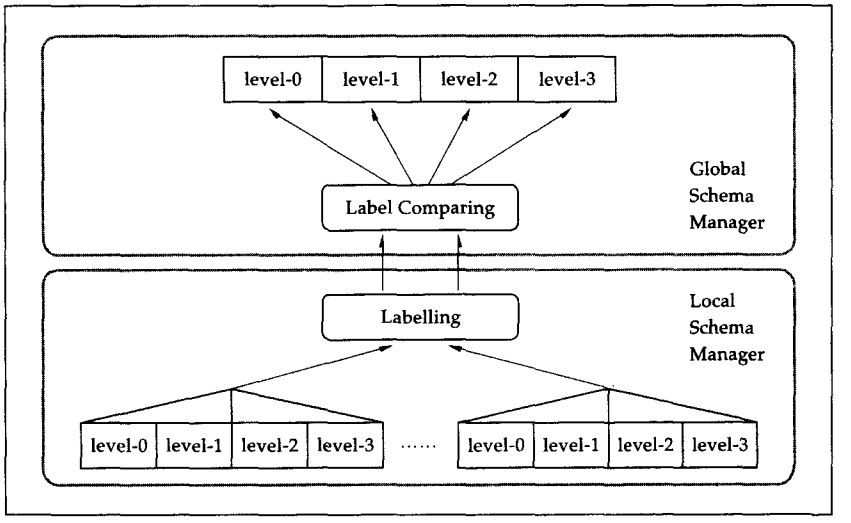
꼬리표에 의해 상위 단계의 스키마 통합과정에서 등급에 기반하여 통합이 이루어질 수 있으며 위의 〔그림 3〕과 같이 표현된다.

스키마 생성 및 삭제시 모든 연산은 결국 전역 스키마 관리자에 의해 이루어진다. 지역 스키마 관리자에 의해 관리되는 스키마는 전역으로 제출시 꼬리표가 부가되며 다음 〔그림 4〕와 같이 표현된다. 스키마 통합은 제출된 스키마가 가지는 등급에 의해 이루어진다. 실제로 사용자는 자신이 가지는 등급보다 상위 단계의 스키마에 대한 검색 권한이 없으므로 실제로 상위의 스키마는 사용자에게 투명한 상태로 보여지게 된다.

위와 같은 기법을 통해 지역 스키마와 전역 스키마간에 보안 등급의 일관성을 유지할 수 있으며 동일한 스키마 상에 존재하는 상이한 등급을 가진 자료객체에 대한 추가적인 연산을 줄일 수 있다.

3.3 스키마의 유지

사용자에게 스키마에 대한 접근이 허용될 때 스키마가 등급의 일관성을 유지하면서 사용자에게 스키마 단위로 검색되기 위해 스키마의 저장 구조가 고려되어야 한다.



〔그림 4〕 지역 스키마를 전역 스키마로 사상

〔표 4〕 저장된 스키마의 형태

LEVEL	SCHEMA	INDEX	ATTRIBUTES
0	SAVINGS0	ACCOUNT-NO	{ NAME, ACCOUNTS }
1	SAVINGS1	ACCOUNT-NO	{ PASSWD }
2	SAVINGS2	ACCOUNT-NO	{ ADDRESS, CREDIT }
3	SAVINGS3	ACCOUNT-NO	{ SOCIAL-SEC-NO }
2	LOAN2	LOAN-NO	{ NAME, ADDRESS }
3	LOAN3	LOAN-NO	{ ACC-CONDITION }
0	INTRO	INTRO-NO	{ SAVING-TYPE }

예로서 스키마는 다음의 〔표 4〕와 같은 형태로 저장되고 관리된다. 등급이 부여된 지역 스키마는 전역 스키마의 일부를 저장하고 전역 스키마는 지역 스키마를 등급에 따라 통합한 형태로 저장한다. 이런 통합된 형태의 저장 구조는 그 보호를 위해 통합된 단위 객체에 따라 보호의 강도가 달라야 한다. 이런 암호화의 강도는 자료객체의 중요도에 따라 달라진다고 할 수 있다.

저축계좌에 대한 스키마를 생성할 때 이를 관리하는 사용자의 등급에 따라 스키마 분할이 이루어지도록 하는 것이다. 원래의 저축계좌는 ACCOUNT-NO, NAME, ACCOUNTS, PASSWD, ADDRESS, CREDIT, SOCIAL-SEC-NO로 구성되어 있을 때 자료객체가 가지는 정보의 질에 따라 다수로 스키마의 분할이 이루어질 수 있다.

스키마 자체가 상이할 경우는 저축계좌와 대출계좌를 예로 들 수 있다. 대출계좌와 같은 경우는 저축계좌와 정보의 질이 다르므로 저축계좌와 상이한 등급을 갖게 된다. 저축 계좌내의 자료 객체 중에서도 대출 계좌와 동일한 등급의 자료는 나타날 수 있으며, 이는 실제로 대출 계좌와 관련있는 자료들이 될 것이다.

모든 스키마는 통합을 위해 색인 부분을 필요로 하며, 실제로 색인을 위한 필드는 그 스키마 상에서 가장 낮은 등급을 가져야 한다. 이는 JOIN 연산을 위해 필요하다.

3.4 자료의 관리

자료는 분산된 형태로 저장되어 있으므로 이를 처리하기 위해 분산된 장소에 대한 정보가 필요하다. 이를 이용하여 분산된 자료의 저장장소를 알 수 있다. Grapevine 시스템[9]에서와 같이 인증과 자료가 저장된 위치에 대한 정보를 제공하기 위해 〔표 5〕와 같은 형태로 정보가 제공된다.

〔표 5〕 자료가 저장된 위치에 대한 정보

등 급	스키마명칭	저 장 정 보
0	savings	d:\\karr\\pro\\s_data00.dat d:\\karr\\pro\\s_data01.dat d:\\karr\\pro\\s_data04.dat
1	savings	d:\\karr\\pro\\s_data10.dat d:\\karr\\pro\\s_data11.dat d:\\karr\\pro\\s_data12.dat d:\\karr\\pro\\s_data13.dat
2	savings	d:\\karr\\pro\\s_data23.dat d:\\karr\\pro\\s_data24.dat d:\\karr\\pro\\s_data20.dat
⋮		

자료객체가 저장된 정보에 대한 보호도 같이 이루어져야 하며 저장된 정보는 자료에 대한 접근을 가능하게 한다. 이들 정보를 이용해 자료에 접근하고자 할 경우 사용자의 인증은 사용자의 등급에 따라 접근 여부가 결정된다.

4. 객체의 보호와 사용자 인증

보호의 대상은 전송되는 자료객체 뿐만 아니라 각 시스템에 저장되어 있는 스키마 정보, 자료 객체, 사용자 정보 등을 들 수 있으며, 제안된 기법에서 이 자료들에 대한 보호는 앞에서 열거했던 방법들로 이루어지며, 궁극적으로는 암호화를 통해 보호가 이루어진다. 사용자 인증은 데이타베이스 사용자가 스키마에 대한 접근 허용 여부를 확인하는 과정이다. 보호되어야 할 스키마의 등급과 사용자의 등급에 대한 비교가 자료객체에 대한 사용자의 접근 허용 여부가 결정된다.

4.1 객체의 보호

사용자의 접근 허용 여부에 따라 실제 자료에 대한 접근은 실제로 시스템간의 통신으로 구성된다. 전송되는 자료의 보호를 위해 서버가 통신 상에서 사용될 키를 관리하는 방법을 사용한 Needham과 Schroeder의 프로토콜과 암호화키와 복호화 키가 상이한 RSA 알고리즘과 같은 암호 기법이 사용될 수도 있다. 사용자에게 알려지지는 않지만 어떤 방식을 사용하느냐에 따라 가용성은 많은 차이를 갖게 된다.

보호를 위한 각 기법은 그 환경을 고려해야 하며 전송이 자주 많이 일어나는 환경에서는 공개키와 같은 기법이 사용되고 전송이 자주 일어나지 않는 환경에서는 키 서버가 키를 관리하는 방법이 더 효율적이다.

공개키 방법은 사용자마다의 키를 생성하는 것이 주기적 혹은 비주기적으로 일어난다는 것을 고려할 때 바람직하지 못한 결과를 낳는다.

키 서버는 키 분배를 위해 더 많은 시간과 더 많은 보안 장치를 필요로 할 것이다. 암호화 기법에 관한 부분은 이 논문의 범위를 벗어나므로 생략한다.

4.2 사용자 인증

사용자 인증은 시스템의 보호를 위해 가장 중요한 과정이다. 여기서 제안한 기법에 적합한 사용자 인증 방법은 다음과 같은 과정을 통해 이루어진다. 첫번째 단계로, 사용자는 시스템 구동시 사용중인 시스템에 대한 자신의 등록 여부를 확인한다. 두번째 단계로서, 사용자는 데이타베이스 시스템에 대한 등록 여부를 확인한다. 두번째 단계로서, 사용자는 데이타베이스 시스템에 대한 등록 여부를 확인할 것이다. 사용자는 사용자 뷰를 생성하거나 미리 생성된 사용자 뷰를 사용하는 과정을 거칠 때마다 사용자가 가진 능력에 따라 비교가 이루어진다.

두번째 단계까지는 사용자가 직접 인지할 수 있는 과정이고 그 후의 단계는 시스템이 수행하는 인증 절차이다. 실제로 시스템에서 이루어지는 인증 절차는 다음과 같다.

[그림 5]의 과정으로 사용자의 객체에 대한 접근 허용 여부를 판단한다. [그림 5]의 과정은 사용자 정보에 포함된 등급을 포함한 Capability와 스키마나 응용 프로그램이 가지는 등급과의 비교를 통해 어떤 등급의 스키마와 응용 프로그램 들이 사용자에게 접근이 허용될지를 결정한다.

5. 구현 및 평가

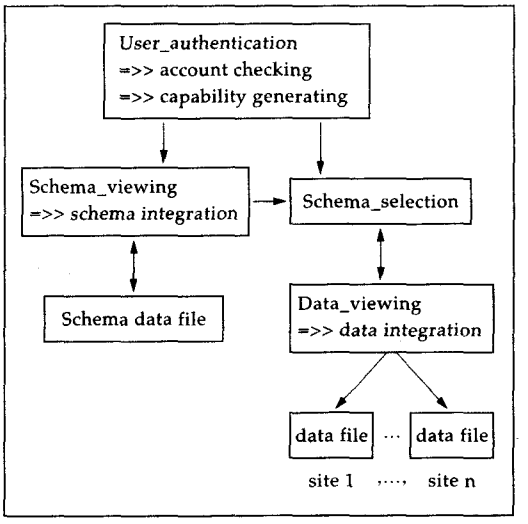
데이타베이스 모델에서 보안을 위한 부가적인 기능은 데이타베이스의 외부 스키마, 개념 스키마, 내부 스키마, 저장 매체간에 등 모든 과정에서 응용될 수 있다. 제안된 기법에서는 내부 스키마와 개념 스키마를 사상시키는 과정과 내부 스키마와 저장매체 같에 자료객체의 입출력 시에 그 기능을 부가한 시스템으로서 이 기법의 결과는 저장매체에서의 자료 분할로 나타나게 된다.

1. DBMS 구동
2. 사용자 계정 확인
   (사용자 등록 여부 및 등급 검색)
3. 다단계 사용자 능력 생성
   (사용자 등급을 부가한 능력의 생성, 사용 중에만 존재)
4. 스키마 검색
   a. 다단계 사용자 능력과 요구된 스키마 검색
      (사용자의 요구에 따라 스키마 브라우징을 위한 전 단계)
   b. 요구된 스키마 검색 및 하위 등급 지향 스키마 통합
      (스키마 지정시 스키마의 통합은 스키마 관리자가 사용자보다 낮은 등급을 가진 하위 스키마를 통합)
5. 자료 검색
   a. 다단계 사용자 능력과 검색될 자료의 등급 비교
   b. 검색될 자료 결정 및 하위 등급 지향 자료 통합

〔그림 5〕 사용자 인증 및 등급에 기반한 스키마와 자료 통합 알고리즘

5.1 보안 데이타베이스 모델

스키마를 이용한 보안 데이타베이스 모델은 네 개의 모듈로 구성된다. 사용자 인증, 스키마 통합, 스키마 선택, 자료 통합의 네개 모듈이다.



〔그림 6〕 시스템의 구성

5.2 사용자 인증의 구현

사용자 인증 방법은 4절에서 제안했던 알고리즘을 이용하며 구현하였으며 실제 보안 데이타베이스 모델 뿐만 아니라 보호를 위한 시스템의 가장 중요한 문제이다. 이는 사용자의 등급과 사용자에게 부여된 계정을 확인하여 다단계 사용자 능력을 구현하는 과정이다. 사용자 정보는 〔그림 7〕과 같이 구성되어 있다.

kim	1
lee	2
kang	0
cho	3

〔그림 7〕 사용자 계정 자료

위의 자료가 구성되어 있을 때 사용자 계정을 입력하여 〔그림 8〕의 과정을 통하여 사용자의 계정과 등급을 확인하게 된다. 이 과정에서 사용자의 암호를 입력하는 부분은 논문의 범위를 벗어나

므로 생략되었다. [그림 7]의 사용자 계정 자료를 이용하여 사용자 다단계 능력을 생성하게 된다. 다단계 능력은 스키마 검색 및 통합시 사용자에 대한 정보를 제공하는 기준인 등급 정보를 유지하는 도구로써 자료에 대한 보호를 다단계로 유지할 수 있다.

```
void user_authentication(char client[10])
{
  while(fscanf(사용자 계정 및 등급) != EOF)
        if(사용자 입력과 사용자 계정 비교)
          사용자 다단계 능력 생성
          // 사용자의 계정을 확인하여 등급 검사 후 사용자가 시스템
             사용 동안 인증을 위한 다단계 능력 생성 //
}
```

[그림 8] 사용자 계정 확인 및 다단계 능력 생성 알고리즘

사용자의 다단계 능력은 사용자가 시스템을 사용하는 동안 계속 유지되며 사용자가 시스템의 사용을 중지할 경우 자동적으로 소거된다. [그림 7]에서와 같이 사용자의 등급에 대한 정보를 유지할 겨우 사용자의 등급을 쉽게 유지할 수 있고 변경이 용이하다는 장점을 갖고 있다.

5.3 스키마의 통합 구현

스키마의 통합을 위해 스키마에 대한 정보는 [그림 9]의 형태로 저장되며 사용자의 등급에 따라 시스템은 스키마의 검색을 통해 동일한 스키마의 상하위의 등급을 검색하여 통합을 하게 된다.

0 3 savings	10 d account_no	15 s name	8 d accounts
1 2 savings	10 d account_no	8 d passwd	
2 3 savings	10 d account_no	20 s address	8 d credit
3 2 savings	10 d account_no	20 d social_sec_no	

[그림 9] 스키마의 저장 형식

위의 정보를 검색할 때 사용자의 등급에 대한 비교가 먼저 이루어지고 이를 통해 동일한 스키마에 대한 상이한 등급의 스키마를 검색하여 통합된 스키마를 생성하게 된다.

[그림 10]의 알고리즘을 통해 사용자 등급에 의한 스키마의 통합이 이루어지며 사용자가 스키마를 검색할 때 스키마에 대한 정보는 하위의 스키마를 통합한 형태이다. 이는 사용자에게 상위의 스키마를 은익시키는 작용을 한다. 스키마를 은익함으로써 사용자는 스키마를 통해 추론할 수 없으며 사용자 자신의 사용자 뷰를 생성할 수 있으므로 시스템 관리자 및 사용자에게 유연성을 제공한다.

```
void schema_browsing(void)
{ while(fscanf(스키마 등급, 스키마 이름) != EOF)
        // 스키마 등급 검색 과정 //
        { 애트리뷰트 읽어들임 ;
          if (사용자등급 == 스키마 등급)
             { viewed_schema에 애트리뷰트를 저장하여 스키마 정보 통합}
             // 하위 지향 스키마 통합 //
        } return;
}
```

〔그림 10〕 스키마 통합 알고리즘

5.4 자료 통합 구현

통합된 스키마를 바탕으로 사용자가 하나의 스키마를 선택하여 하나의 자료객체에 접근하고자 할 때 분할된 상태로 있는 자료객체를 통합하여 사용자에게 보여주게 된다. 사용자는 통합된 스키마 내에서만 자료에 대한 연산이 가능하다.

```
void data_browsing()
    i = 사용자 등급;
       // i 값을 사용자 등급으로 할당 //
{ while(fscanf(자료의 저장 화일명) != EOF)
        // 자료 화일 검색 과정 //
           while (fscanf(분할된 자료) != EOF)
           viewed_data에 자료를 저장하여 자료 통합;
        // 하위 지향 자료 통합 //
       i--;
        // 하위 등급 자료 화일을 검색하기 위해 i 값을 1 감소 //
}
```

〔그림 11〕 자료 통합 알고리즘

〔그림 11〕의 알고리즘을 통해 각 지역 DBMS로 분산된 자료의 통합을 할 수 있으며 지역과 전역간의 자료 등급의 일관성을 쉽게 유지할 수 있다. 분할된 자료에 대한 통합은 시스템에게 자신의 지역 DBMS에 존재하지 않는 자료에 대한 요구를 상대적으로 감소시키므로 통신량을 줄일 수 있다.

5.5 정성적 평가

Seaview 모델에서 제시한 polyinstantiation 기법과 CDT 모델에서 제안한 범위값을 이용한 기법은 레코드나 레코드 내의 필드 단위로 보안 등급이 할당됨으로써 사용자에게 자료객체가 투명하게 제시되지는 않는다.

schema						
account-no	name	accounts	passwd	address	credit	[redacted]
11-11-11	kang	1000000	3312	서울 성북	5000	[redacted]
{ 색인부분 }	{ 등급 0 }		{ 등급 1 }	{ 등급 2 }		{ 등급 3 }

〔그림 12〕 레코드 내의 필드 단위로 등급 할당

〔그림 12〕에서와 같이 스키마 내의 각 필드가 갖는 값이 사용자의 등급과 다른 등급을 갖는 경우 사용자 등급 1을 가진 사용자가 시스템 관리자가 제공한 사용자 뷰를 사용할 경우 사용자에게 검색되는 자료는 레코드 중 일부만이 사용자가 인지할 수 없는 상태로 보여지게 될 것이다. 투명한 상태로 자료가 제공되지 않으므로 사용자는 자신이 접근할 수 없는 자료 객체에 대하여 인지할 수 있다.

savings						
account-no	name	accounts	passwd	address	credit	[redacted]
11-11-11	kang	1000000	3312	서울 성북	5000	[redacted]
등급 0						
등급 1						
등급 2						
등급 3						

〔그림 13〕 분할된 스키마 단위로 등급이 할당된 경우

〔그림 13〕과 같이 등급별로 분할된 스키마를 이용할 경우 시스템 관리자는 사용자 뷰를 사용자의 유형을 고려하여 생성함으로서 사용자 뷰를 통한 접근제어를 얻을 수 있다. 사용자가 자신이 정의한 사용자 뷰를 사용할 경우 사용자가 접근할 수 있는 스키마가 〔그림 13〕에서와 같이 제한되므로 사용자는 자신이 원하는 자료객체를 허용된 스키마 내에서 접근할 수 있다. 스키마를 이용한 보안 모델에서는 자료 접근 단계에 있어서 접근 취소가 발생하지 않는 것이다. 사용자에게 스키마는 투명한 상태로 제공된다. 전체 자료가 아닌 필요한 자료만이 검색되므로 통신량을 줄일 수 있다. 스키마를 이용한 보안 모델에서는 통계 데이타베이스와 달리 보호하기 위한 자료객체의 내용을 제한하지 않고 자료객체에 대한 접근을 허용한다. 보호의 필요성이 있는 자료객체에 대해서만 접근을 제어함으로써 통신량을 줄일 수 있다.

6. 결 론

이 논문에서 스키마 통합과 분할을 이용해서 자료객체의 보호를 달성하는 기법을 제안했다. 분할된 스키마 단위로 등급이 부여되고 상위 등급의 스키마는 사용자에게 은폐되는 기법이다. 사용자는 다단계로 보안 등급이 분류된 능력을 갖게되며 객체에 대한 접근이 시도될 때마다 사용자의 능력과 객체에 대한 비교가 이루어진다. 지역에서 만들어진 스키마를 등급을 부여하는 협상의 과정을

거쳐 전역으로 제출하여 통합이 이루어진다. 스키마를 이용한 기법을 통해서 지역과 전역에서의 스키마와 자료객체의 일관성을 쉽게 유지할 수 있으며, 분산환경에서 DBMS의 문제점인 스키마의 생성과 변경, 삭제를 용이하게 할 수 있다. 스키마를 이용한 데이타베이스 보안 모델은 접근이 허용되지 않는 스키마를 사용자에게 제공하지 않으므로 기존의 기법에서 발생하는 문제점인 자료 접근 단계에서 발생하는 자료객체에 대한 과도한 접근 취소를 줄일 수 있고 추론의 가능성을 배제할 수 있다. 전역 데이타베이스 시스템과 지역 데이타베이스 시스템간에 발생하는 과다한 접근 취소와 불필요한 동작을 줄임으로서 security sharing의 정도를 높일 수 있다. 보호할 필요성이 있는 스키마를 사용자에게 은익함으로써 사용자는 자신의 등급에 따라 통합된 사용자 뷰를 생성할 수 있으며 시스템 관리자는 사용자에게 미리 정의된 사용자 뷰를 제공할 수 있는 유연성을 제공한다.

향후의 연구는 각 등급의 스키마 내에 존재하는 다른 등급의 자료객체를 처리하기 위한 기법의 연구와 이를 처리하는데 적합한 보안정책에 대한 연구가 계속되어야 한다.

참 고 문 헌

[1] 김영호, 유헌창, 허용도, 손진곤, 황종선, "정보보호를 위한 능력의 선택적 및 부분적 취소", 정보과학회 추계논문집, pp. 685-688, 1993.

[2] Jennifer Seberry and Josef Pieprzyk, *Cryptography: An Introduction to Computer Security*, Prentice Hall, pp. 233-245, 1989

[3] Andrzej Goscinski, *Distributed Operating Systems*, Addison Wesley Publishing company, 1991

[4] D.E. Denning, T.F. Lunt, R.R. Schell, W.R. Shockley, and M. Heckman "The SeaView Security model," IEEE Symposium on Security and Privacy, pp. 218-233, 1988

[5] Lt.Gregory, S.Hoffenstand, and David K. Hsiao, "Secure Access Control with high Access precision," IFIP Trans. A : Computer Science and Technology, Database Security Ⅱ Status and Prospets, pp. 167-176, 1990

[6] Seog-Jun Kang, Chan-Yeol Park, Chong-Sun Hwang, "A Database Security Based on the Schema Partition and the Integration in Distributed Environments," ICCTA, Proceedings of the First International Conference on Computer Technology and Applications, pp.80-85, 1994

[7] 안미림, 유헌창, 황종선, "접근제어에서 다단계 보안 개념의 적용을 위한 확장된 능력", 정보과학회 춘계 논문집, pp. 373-376, 1994

[8] Richard Y.Kain, "On Access Checking in Capability-Based Systems," IEEE Transactions on Software engineering, Vol 1., SE-13, NO.2, Feb. 1987

[9] George F. Coulouris, Jean Dollimore, *Distributed Systems*, Addison Wesley Publishing company, pp. 321-346, 1988

[10] Matthew Morgenstern, Teresa F. Lunt, Bhavani Thuraisingham, and David L. Spooner, "Security issues in

federated database systems," IFIP Trans. A : Computer Science and Technology, Database Security V Status and Prospets, pp. 131-148, 1992

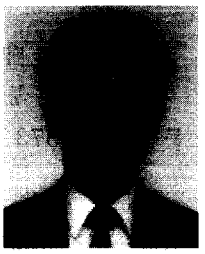
[11] Gray W. Smith, "Solving Multilevel Database Security Problems : Technology Is Not Enough," IFIP Trans. A : Computer Science and Technology, Database Security Ⅲ Status and Prospets, pp. 115-125, 1990

□ 著者紹介

강 석 준

1989년 전남대학교 전산통계학과 학사 취득
1995년 고려대학교 대학원 전산학 석사 취득
1995년 현재 고려대학교 대학원 전산학 박사과정

※ 관심분야 : 데이타베이스 보안, 분산시스템, 데이타 통신



김 용 원

1986년 고려대학교 수학과 학사 취득
1988년 고려대학교 대학원 전산학 석사 취득
1993년 8월 고려대학교 대학원 전산과학과 박사 수료
1995년 현재 건양대학교 정보관리학과

※ 관심분야 : 분산데이타베이스, 데이타 보안, 알고리즘

황 종 선

1966년 고려대학교 수학과 학사 취득
1968년 고려대학교 대학원 석사 취득
1978년 Univ. of Georgia 박사 취득
1994년 현재 고려대학교 전산과학과 교수

※ 관심분야 : 알고리즘, 분산 시스템, 데이타 보안