다단계 보안을 위한 확장 릴레이션의 운영 의미론

조 완 수† 배 해 영††

요 약

본 논문에서는 다단계 보안을 지원하는 관계 데이타베이스 관리 시스템을 설계하기 위하여 표준 관계 모델을 확장하고, 새로운 다단계 무결성 제약조건을 제시하며, 이를 지원하는 다단계 릴레이션의 운영 의미를 제시한다. 확장된 관계 모델과 새로운 무결성 제약조건은 다단계 데이타베이스를 일관된 상태로 유지시키며, 다중사례를 지원하면서 이의 허용에 따른 엔티티 및 관계 표현의 모호성을 제거할 수 있는 기반을 제공한다. 확장된 다단계 릴레이션에 대한 다단계 갱신 연산은 서로 다른 보안 분류의 요소를 동시에 처리할 수 있는 다단계 입력 및 갱신 트랜잭션을 지원하여 갱신 연산의 효율성을 증가시킨다. 또한 다단계 릴레이션의 분해를 위한 알고리즘 구현의 기초를 제시한다.

The Operational Semantics of Extended Relations for Multilevel Security

Wan-Soo Cho† Hae Young Bae††

ABSTRACT

In order to design an extended relational database management system supporting multilevel security, the standard relational data model is extended and new relational integrity constraints are proposed for the model. The extended relational model and proposed multilevel integrity constraints maintain database in consistent state and produce a basis that can eliminate ambiguity of entity and relationship representations by polyinstantiation. The proposed update semantics can increase the efficiency of update operations by supporting multilevel entry and updates. The semantics also provides a basis for the implementation of decomposition of extended relations.

1. 서 론

데이타베이스 보안은 데이타베이스 내의 데이타에 대한 인가되지 않은 접근, 의도적인 변경이나 파괴 및 데이타의 일관성을 저해하는 사고 등으로부터 데이타를 보호하는 것이다. 대부분의 데이타베이스 시스템은 보안 대책으로 데이타에 대한 사용 권한을 제어하는 접근 제어를 채택하고 있으나 이는 운영체제를 위한 보안 요구를 반영한 것으로 데이타베이스에 대해서는 적용이 부적합하다[1]. 접근 제어를 위한 보안 정책은 임의적 접근 제어와 강제적 접근 제어로 구분된다. 임의적 제어는 주체나 주체가 속해 있는 그룹의 식별자를 근거로 엔티티에 대한 접근을 제한하는 방식이며, 강제적 제어는 엔티티에 포함된 정보의 비밀 등급과 주체에 부여된 비밀 취급 인가를 기반으로 엔티티에 대한 접근을 제어하는 방식이다. 강제적 접근 제어는 다단계 보안의 구현을 위한 방법론의 핵심이 된다.

본 논문에서는 필드 수준에서의 다단계 보안을 지원하는 관계 데이타베이스 시스템을 설계하기 위하여 관계 모델을 확장하고, 확장된 관계 모델을 위한 무결성 제약조건을 제시하며, 이에 따른

† 정 회 원 : 국방정보체계연구소 선임연구원
†† 종신회원 : 인하대학교 전자계산공학과 교수
논문접수 : 1995년 7월 1일, 심사완료 : 1995년 12월 20일.

다단계 릴레이션의 운영 의미를 제시한다.

2. 다단계 관계 데이타 모델

다단계 보안을 지원하는 관계 데이타베이스 시스템을 구축하기 위한 많은 연구가 진행되어 왔으나 다단계 관계 모델의 정의에 대해서는 아직 일치가 되지 않고 있다. 다단계 관계 모델의 특징은 다단계 데이타에 관련되는 실세계의 운영 요구에 의하여 결정된다. 이러한 요구사항은 일반적으로 강제적 보안, 원자 사실의 분류(classification), 다단계 뷰, 다단계 입력 및 갱신, 각 등급에서의 일관성 유지 및 접근 등급에 기초한 검색 등의 특징을 지닌다.

본 논문의 표기는 다음과 같다: A_i은 사용자가 지정하는 기본 키이고 C_i은 A_i의 보안 분류이다. $t[A_i]$는 투플 t의 A_i 애트리뷰트의 값을 나타내며, $t[C_i]$는 C_i 애트리뷰트의 값을 표현한다. 투플 등급이 c인 투플을 c-투플이라고 하고 접근 등급이 c인 주체는 c-주체라고 한다. 또한 접근 등급 c에서의 인스턴스는 c-인스턴스라고 한다. 접근 등급의 집합은 지배(dominate)라고 불리는 부분 순서 관계 $\geq$를 갖는 속(lattice)으로써 구조화되며, 단순 보안 속성과 제한 ★-속성의 두 가지 규칙으로 접근 요구사항을 규정한다[2].

2.1 다단계 릴레이션

다단계 데이타를 처리하기 위해서는 필드 수준에서 분류 레이블이 포함되도록 릴레이션을 확장하여야 한다. 그러나 기존의 필드 수준 보안 분류 모델[3, 4, 5, 6]은 엔티티 및 관계 표현에서 모호성이 존재하는 문제점을 내포하고 있는데, 이를 해결하고 다단계 릴레이션의 모델링 능력과 다단계 트랜잭션의 처리 효율성을 높이기 위하여 투플 수준 보안 분류 모델의 특성을 혼합한 하이브리드 모델을 고려하여야 한다[13]. 하이브리드 모델에서의 다단계 릴레이션은 다음의 두 부분으로 구성된다.

[정의 1] 상태 불변의 다단계 릴레이션 스킴, $R(A_1, C_1, \cdots, A_n, C_n, TC)$. A_i는 도메인 D_i의 데이타 애트리뷰트이며, C_i는 A_i에 대한 분류 애트리뷰트이고, TC는 투플 등급 애트리뷰트이다. C_i의 도메인은 접근 등급 속의 부속(sublattice)을 지정하는 쌍$[L_i, H_i]$으로 정의된다. 이때 $L_i \leq H_i$이다.

[정의 2] 속의 각 접근 등급 c에 하나씩 존재하는 상태 종속의 릴레이션 인스턴스 R_c의 집합, $R_c(A_1, C_1, \cdots, A_n, C_n, TC)$. 각 인스턴스는 별개의 투플 $(a_1, c_1, \cdots, a_n, c_n, tc)$의 집합이며, $a_i \in D_i$ 혹은 a_i 널이고, $c \geq c_i$이며, $tc = \text{lub}\{c, c_i : i = 1..n\}$이다. 또한 a_i가 널이 아니면 $c_i \in [L_i, H_i]$이다. a_i가 널이면 c_i는 기본 키의 등급으로 분류된다. lub는 최소상한치(least upper bound)를 의미한다.

투플 등급을 [정의 2]와 같이 정의하면 c-주체는 c-투플의 개별적인 분류 애트리뷰트에 ★-속성을 위반하지 않는 범위 내에서 값을 지정할 수 있다. 따라서 c-주체에 의한 투플 등급의 값 지정은 금지되어야 한다. 기존의 다단계 관계 모델[4, 5, 6, 7, 8, 9, 10]에서는 주체가 분류 값을 명시적으로 지정하는 것을 지원하지 않는 대신 c-주체에 의해 갱신되는 투플의 모든 분류 값을 c로 자동 설정하기 때문에 다단계 입력 및 갱신을 지원하지 못한다. 또한 c-주체에 의해서 삽입 및 갱신되는 모든 투플은 $tc = \text{lub}\{c_i : i = 1..n\}$를 만족시켜야 한다. 이는 특히 높은 등급의 주체의 관점에서 볼 때 다단계 릴레이션의 모델링 능력을 제한하는 것으로 서비스의 가용성을 저하시키거나, 하나의 입력을 위하여 복수의 트랜잭션을 수행해야 하는 비효율성을 야기시킨다. 또한 다단계 데이타에 대한 올바른 보안 분류나 일관성 있는 보안 분류를 효율적으로 지원하지 못한다[13].

2.2 다단계 무결성 제약조건

다단계 관계 모델에서는 등급별로 서로 다른 인스턴스가 제공되기 때문에 각 등급의 데이타 일관성을 보장하기 위하여 무결성 제약조건을 확장하거나 새로운 제약조건을 정의하여야 한다[13].

2.2.1 다단계 엔티티 무결성

다단계 관계 모델에서는 인스턴스가 투플의 단

일 집합이 아닌 등급별 투플 집합의 집합체로 정의되기 때문에 함수적 종속성이 모호해지므로 엔티티 무결성을 확장하여야 한다.

[정의 3] R_c는 모든 $t \in R_c$에 대하여 다음이 충족될 때 다단계 엔티티 무결성을 만족시킨다.

1. $A_i \in A_1 \Rightarrow t[A_i] \neq$ 널,
2. $A_i, A_j \in A_1 \Rightarrow t[C_i] = t[C_j] = t[C_1]$,
3. $A_i \notin A_1 \Rightarrow t[C_i] \geq t[C_1]$.

2.2.2 인스턴스간 무결성

투플 등급이 $tc > \text{lub}\{c_i : i = 1..n\}$인 투플의 삽입을 c-주체에게 허용하면서 ★-속성을 보장하기 위해 투플 등급에 기초하여 인스턴스간 무결성을 새로이 정의한다.

[정의 4] R_c와 $R_{c'}$는 R의 인스턴스이며, $c \geq c'$이다. $R_{c'} = \sigma(R_c, c')$가 성립할 때 R은 인스턴스간 무결성을 만족시킨다. σ는 여과 함수로서 다음과 같이 R_c로부터 $R_{c'}$을 생성한다.

1. 모든 $t \in R_c$에 대하여 다음이 성립되는 $t' \in R_{c'}$이 존재한다 : $R_{c'} \{t \in R_c \mid t[TC] \leq c'\}$
2. $R_{c'}$의 모든 투플은 상기의 규칙에 의해서만 유도된다.

2.2.3 투플 포함 무결성

투플 포함 무결성은 투플 등급의 확장에 따른 ★-속성의 위반을 방지하기 위한 새로운 제약조건이다.

[정의 5] R_c는 모든 t, $s \in R_c$에 대하여 다음이 만족될 때 투플 포함 무결성을 만족시킨다.

1. 모든 A_i에 대하여, $t[A_i, C_i] = s[A_i, C_i]$이면서 $t[TC] > s[TC]$이면 s는 t를 포함한다고 정의한다.
2. 임의의 R_c에는 포함 관계에 있는 두 개의 투플이 존재하지 않아야 한다.

2.2.4 다중사례 무결성

다중사례(polyinstantiation) 무결성은 비합리적인 인스턴스의 발생을 억제하기 위하여 다단계 릴레이션의 애트리뷰트간에 정의된다. 기존의 다단계 관계 모델은 상이한 다중사례 무결성 제약조건을 제시하고 있다. [4]는 FD 다중사례 무결성(PI-FD)과 MVD 다중사례 무결성(PI-MVD)을, [5]에서는 PI-FD와 NULL 다중사례 무결성(PI-NULL)을, [11]에서는 PI-FD와 동적 PI-MVD(PI-DMVD)를, [6, 9]에서는 PI-FD와 TC 다중사례 무결성(PI-TC)을 필요한 조건으로 제안하였으나 공통적인 제안의 근거는 존재하지 않는다. 본 절에서는 이들 제약조건을 엔티티에 대한 일관성 있는 정보 제공 능력과 릴레이션간의 참조에 따른 모호성 제거의 관점에서 분석한다[13]. 이들에 대한 상세한 정의는 [13]에 제시되어 있다.

PI-FD는 다단계 릴레이션의 진정한 기본 키를 정의하는 기반을 제공해 주고, PI-TC는 각 등급별로 실세계의 엔티티에 대한 일관성 있는 실체를 제공해 주는 무결성 제약조건이다. 반면에 PI-MVD와 PI-DMVD, PI-NULL은 지나치게 제한적이거나 의미가 불투명한 투플의 생성을 유발하게 되어 사용자에게 정확한 정보를 전달하지 못하게 되고, 또한 참조의 모호성을 유발하게 된다. 따라서 PI-MVD, PI-DMVD, PI-NULL은 다단계 릴레이션의 다중사례 무결성 제약조건에서 삭제하여야 한다.

2.2.5 다단계 참조 무결성

다단계 릴레이션의 참조는 참조하는 투플과 참조되는 투플의 등급별 관계에 따라 신호 채널이 존재할 수 있고, 다중사례에 의하여 참조 모호성이 발생할 수 있다. 참조하는 릴레이션 R의 외부 키를 FK라고 하고 참조되는 릴레이션 Q의 대응되는 기본 키를 PK라고 하면 다단계 엔티티 무결성에 의해 외래 키도 역시 균등하게 분류되어야 한다.

[정의 6] R은 모든 R_c와 $t \in R_c$에 대하여 다음이 충족될 때 다단계 외래 키 무결성을 만족시킨다.

1. $(\forall A_i \in FK)[t[A_i] =$ 널] 혹은 $(\forall A_i \in FK)[t[A_i] \neq$ 널]이 항상 성립한다.
2. $A_i, A_j \in FK \Rightarrow t[C_i] = t[C_j]$.

본 논문에서는 투플의 투플 등급간 상호 관계를 고려하여 신호 채널을 발생시키지 않는 다단계 참조 무결성을 정의한다. 특히 릴레이션간의 참조에 대한 일관성을 유지하기 위해 식별된 투플 갱신 연산의 규칙[12]을 이용하여 투플 등급

별 관계에 따라 이들 규칙이 다단계 릴레이션에 미치는 영향을 파악하고, 이를 근거로 다단계 참조 무결성을 정의한다.

[정의 7] R과 Q는 R_c와 Q_c에서, $t[FK] \neq$ 널인 모든 $t \in R_c$에 대하여 다음을 만족시키는 $q \in Q_c$가 존재하고 갱신 연산 규칙이 다음을 만족시킬 때 다단계 참조 무결성을 만족시킨다.

1. $t[FK]=q[PK]$,
2. $t[TC]<q[TC]$이면, 제한 삭제 규칙과 제한 갱신 규칙만이 적용 가능하며 이외의 모든 규칙은 적용 불가능하다.
3. $t[TC]=q[TC]$이면, 모든 규칙이 적용 가능하다.
4. $t[TC]>q[TC]$이면, 제한 삭제 규칙과 제한 갱신 규칙만이 적용 불가능하며 이외의 모든 규칙은 적용 가능하다.

2.3 다단계 관계 모델의 분석

본 논문의 다단계 관계 모델은 기존의 모델과 비교할 때 다음과 같은 차이를 보인다.

첫째, 투플 등급의 확장으로 주체는 분류 값을 지정할 수 있게 된다. 따라서 단일 트랜잭션으로 다단계 입력 및 갱신을 수행할 수 있게 되어 갱신 연산의 효율성이 증가하게 되었다. 둘째, 인스턴스간 무결성을 투플 등급에 기초하여 재 정의함으로써 불필요한 널 값의 도입을 억제하였다. 셋째, 투플 등급의 정의 확장에 따라 투플 포함 무결성을 새로이 제안하였다. 넷째, PI-FD와 PI-TC의 조합을 다중사례 무결성 제약조건으로 정의하여 다단계 참조 모호성을 제거할 수 있는 기반을 제공하였다. 다섯째, 다단계 참조 무결성 제약조건을 제안하였다.

3. 다단계 릴레이션의 운영 의미

다중사례는 다중사례 엔티티(entity polyinstantiation)와 다중사례 요소(attribute polyinstantiation) 형태로 발생한다. 다중사례 엔티티는 실세계의 상이한 엔티티를 표현하며, 다중사례 요소는 동일한 엔티티를 표현한다. 다중사례에 대한 해석은 다단계 관계 이론의 일부를 구성하는 것으로, 다단계 릴레이션의 운영 의미를 정의하는 근거로 사용되어야 한다[11]. 다단계 시스템의 보안을 담당하는 정보보안베이스(Trusted Computing Base)의 분할 및 보안 메카니즘으로써의 뷰의 사용에 의한 다단계 보안 데이타베이스 시스템 설계 방법[3, 4]을 택하면 다단계 릴레이션은 표준 릴레이션 상의 뷰로써 구현되는데, 이러한 다단계 릴레이션, 즉 뷰의 갱신 가능성을 보장하기 위하여 다단계 릴레이션을 표준 릴레이션으로 분해 및 복구하는 알고리즘을 개발하여야 한다. 본 논문에서 제안한 다단계 릴레이션의 운영 의미는 다단계 릴레이션의 분해 및 복구 알고리즘의 기초가 된다.

다단계 릴레이션의 기본 연산을 정의할 때 고려하여야 할 사항은 다음과 같다 : 첫째, 표준 관계 데이타베이스 시스템의 운영 의미와 가능한 한 가깝도록 정의하여야 한다. 둘째, 다단계 데이타에 대한 보안 요구를 반영하여야 한다. 셋째. 데이타 분류에 의한 사용자의 선택 기준 지정을 허용하여야 한다. 넷째, 다단계 처리를 지원하여야 한다. 다섯째, 모든 다단계 무결성 제약조건을 만족시켜야 한다.

3.1 다단계 운영 의미의 해석

c-주체는 R_c에 대하여 갱신 연산을 수행한다. c-주체의 관점에서 볼 때 R의 다른 인스턴스들은 그 등급에 따라 세 가지로 구분될 수 있다[7]. 즉, c를 지배하는 등급에서의 인스턴스 $R_{c'>c}$, c에 의해 지배되는 등급에서의 인스턴스 $R_{c'<c}$ 및 c와 지배 관계에 있지 않기 때문에 비교할 수 없는 등급에서의 인스턴스 $R_{c'\sim c}$ 등으로 구분된다. ★-속성에 의해서 c-주체는 $R_{c'<c}$이나 $R_{c'\sim c}$에 대해서는 갱신 연산을 수행할 수 없다. 따라서 c-주체에 의한 연산 수행은 투플 등급이 c인 R_c의 투플에 대해서만 적용되어야 하며 이들 투플에 대한 변경은 $R_{c'>c}$에 반영되어야 한다. $R_{c'>c}$에의 반영은 $R_{c'>c}$에 새로운 투플의 삽입이나 기존 투플의 갱신 혹은 삭제를 요구하게 된다.

3.2 삽입 연산의 운영 의미

c-주체에 의한 삽입 문장의 일반 형식은 다음과 같다. 표기에서 직각 괄호 "[ ]"는 해당 항목이

선택적임을 의미하며, "…"은 반복을 표시한다.

INSERT
INTO $R_c[(A_i[[, C_i], A_j[, C_j]] \cdots)]$
VALUES $(a_i[[, c_i], a_j[, c_j]] \cdots)$;

C_i는 명시적으로 값이 주어질 수도 있으며, 생략되는 경우에는 c로 자동 설정된다. 투플 t의 삽입이 허용되기 위해서는 t가 다단계 엔티티 무결성을 유지하면서 R_c에 존재하지 않는 새로운 엔티티를 나타내던가 즉, 동일한 기본 키 값이 존재하지 않거나 다중사례 엔티티를 표현하는 투플이어야 하며, 다중사례 요소인 경우에는 PI-FD와 PI-TC를 만족하여야 한다. 또한 R_c가 릴레이션 Q_c와 참조 관계를 이루고 있다면 다단계 참조 무결성을 만족하여야 한다. 따라서 R_c에 대한 t의 삽입은 다음의 조건이 만족되는 경우에 허용이 된다.

(1) $t[A_1]$에 널이 존재하지 않으며, 모든 A_i, $A_j \in A_1$에 대하여 $t[C_i]=t[C_j]=t[C_1]$이고, 모든 $A_i \notin A_1$에 대하여 $t[C_i] \geq t[C_1]$가 성립된다.

(2) 모든 $u \in R_c$에 대하여,

① $t[A_1] \neq u[A_1]$이거나,

② $t[A_1]=u[A_1]$이면 $t[C_1] \neq u[C_1]$이거나,

③ $t[A_1, C_1]=u[A_1, C_1]$이면, $t[TC]>u[TC]$이고, 모든 $A_i \notin A_1$에 대하여, $t[A_i] \neq u[A_i]$이면 $t[C_i] \neq u[C_i]$가 성립된다.

(3) R_c가 Q_c에 대한 외래 키 FK를 갖는다면,

① 모든 $A_i \in FK$에 대하여 $t[A_i]$=널 혹은 $t[A_i] \neq$널이고,

② 모든 A_i, $A_j \in FK$에 대하여 $t[C_i]=t[C_j]$이며,

③ $q \in Q_c$에 대하여, $t[FK]=q[A_1]$이고 $t[C_{FK}]=q[C_1]$이면서 $t[TC] \geq q[TC]$가 성립된다.

이상의 조건이 만족되어 t가 R_c에 삽입되면 모든 $R_{c'>c}$에도 t가 삽입되고 $R_{c'>c}$는 투플 포함 무결성을 만족시켜야 한다.

3.3 갱신 연산의 운영 의미

c-주체에 의한 갱신 문장의 형식은 다음과 같다. 조건에는 데이타에 대한 지정뿐만 아니라 분류에 대한 지정도 포함될 수 있다.

UPDATE R_c
SET $A_i=a_i[[, C_i=c_i], A_j=a_j[, C_j=c_j]] \cdots$
[WHERE 조건];

다중사례에 의해 투플이 등급별로 다른 값을 갖는 보안 종속 필드와 모든 등급에서 동일한 값을 갖는 보안 독립 필드를 갖는 경우 갱신이 어려워진다. 보안 종속 필드의 갱신은 해당 등급에서만 영향을 미치는 단일 단계 연산으로 수행이 간단하지만, 보안 독립 필드의 갱신은 데이타의 불일치가 발생하지 않도록 하여야 한다. 또한 갱신에 따른 정보 흐름을 방지하기 위하여 투플 등급이 주체의 접근 등급과 동일한 경우에만 갱신이 허용되어야 한다. 조건을 만족시키는 투플의 투플 등급이 주체의 접근 등급보다 낮은 경우에는 ★-속성을 만족시키기 위하여 다중사례를 발생시키는 추가의 투플을 삽입시켜야 한다. 다단계 참조 무결성을 유지하기 위해서는 적합한 갱신 규칙을 선별적으로 적용하여야 한다. 조건을 만족시키는 t의 갱신은 다음의 조건을 만족시켜야 한다.

(1) $t[TC]=c$인 t가 존재하는 경우, t를 다음의 t'로 대체한다 : $A_k \in$SET 절이면 $t'[A_k, C_k]=(a_k, c_k)$이고, $A_k \notin$SET 절이면 $t'[A_k, C_k]=t[A_k, C_k]$이다.

① $t[A_1]$에 널이 존재하지 않으며, 모든 A_i, $A_j \in A_1$에 대하여 $t'[C_i]=t'[C_j]=t'[C_1]$이고, 모든 $A_i \in A_1$에 대하여 $t'[C_i] \geq t'[C_1]$가 성립된다.

② $t'[A_1, C_1]=u[A_1, C_1]$이 만족되는 모든 $u \in R_c$와 모든 $A_i \notin A_1$에 대하여, $t'[A_i] \neq u[A_i]$이면 $t'[C_i] \neq u[C_i]$가 성립된다.

(2) $t[TC]<c$인 t만 존재하는 경우, t를 변화시키지 않으면서, 다음의 t''를 R_c에 삽입한다 : $A_k \in$SET 절이면 $t''[A_k, C_k]=(a_k, c_k)$이고, $A_k \notin$SET 절이면 $t''[A_k, C_k]=t[A_k, C_k]$이다.

① $t''[A_1]$에 널이 존재하지 않으며, 모든 A_i, $A_j \in A_1$에 대하여 $t''[C_i]=t''[C_j]=t''[C_1]$이고, 모든 $A_i \notin A_1$에 대하여 $t''[C_i] \geq$

$t''[C_i]$가 성립된다.

② $t''[A_i, C_i]=u[A_i, C_i]$이 만족되는 모든 $u\in R_c$와 모든 $A_i\in A_i$에 대하여, $t''[A_i]\neq u[A_i]$이면 $t''[C_i]\neq u[C_i]$가 성립된다.

③ $t''[A_i, C_i]=u[A_i, C_i]$이 만족되는 모든 $u\in R_c$에 대하여, $t''[TC]\neq u[TC]$가 성립된다.

(3) Q_c가 R_c의 기본 키 A_i에 대한 외래 키 FK를 갖고 $q[FK]=t[A_i]$인 $q\in Q_c$가 존재하며 A_k(∈SET절)$\in A_i$이라 한다면, $q[C_{FK}]=t[C_i]$을 만족하는 $q\in Q_c$와 $t\in R_c$에 대하여,

① $q[TC]>t[TC]$이면, 연쇄 갱신 규칙과 널화 갱신 규칙만이 적용 가능하다.

② $q[TC]=t[TC]$이면, 모든 갱신 규칙이 적용 가능하다.

③ $q[TC]<t[TC]$이면, 제한 갱신 규칙만이 적용 가능하다.

R_c에서의 갱신이 성공하면 갱신 내용을 다음과 같이 $R_{c'>c}$에 반영하여야 한다.

(1) $t[TC]=c$인 $t\in R_c$가 존재하여 t를 t'로 대체한 경우,

① $t\in R_{c'>c}$를 다음의 t'로 대체한다 : $A_k\in$ SET 절이면 $t'[A_k, C_k]=(a_k, c_k)$이고, $A_k\notin$SET 절이면 $t'[A_k, C_k]=t[A_k, C_k]$이다.

② 모든 A_k(∈SET절)에 대하여, $u[A_i, C_i]=t[A_i, C_i]\wedge u[A_k, C_k]=t[A_k, C_k]$를 만족하는 $u\in R_{c'>c}$가 존재하면 $u[TC]>c$인 u에 대해서만 u를 다음의 u'으로 대체한다 : $A_k\in$SET 절이면 $u'[A_k, C_k]=(a_k, c_k)$이고, $A_k\notin$SET 절이면 $u'[A_k, C_k]=u[A_k, C_k]$이다.

(2) $t[TC]<c$인 t만이 존재하여 t''가 R_c에 삽입된 경우, t''를 $R_{c'>c}$에 삽입한다.

(3) 모든 t, $s\in R_{c'>c}$와 $i=1..n$에 대하여, $t[A_i, C_i]=s[A_i, C_i]$이고 $t[TC]<s[TC]$인 t와 s가 존재하면 t는 s를 포함한다. 따라서 s는 삭제되고 t만이 $R_{c'>c}$에 존재하게 된다.

3.4 삭제 연산의 운영 의미

c-주체에 의한 삭제 문장은 다음과 같은 형식을 지니게 된다.

```
DELETE
FROM    Rc
[WHERE  조건];
```

삭제 연산은 ★-속성에 의하여 조건을 만족시키는 투플의 투플 등급이 c인 투플만을 삭제하여야 한다. 삭제되는 투플과 다중사례 요소인 투플도 삭제되어야 하며, t로 표현되는 엔티티를 나타내는 모든 투플을 $R_{c'>c}$로부터 삭제하여야 한다. 또한 다단계 참조 무결성 제약조건에 의하여 삭제 규칙을 선별적으로 적용하여야 한다. 따라서 c-주체에 의한 t의 삭제는 다음의 조건을 만족시켜야 한다.

(1) $t[TC]=c$인 t를 R_c에서 삭제한다.

(2) 모든 $u\in R_{c'>c}$에 대하여 $t[A_i, C_i]=u[A_i, C_i]$이고 $u[TC]\geq c$인 u를 $R_{c'>c}$에서 삭제한다.

(3) Q_c가 R_c의 기본 키 A_i에 대한 외래 키 FK를 갖고 $q[FK]=t[A_i]$인 $q\in Q_c$가 존재한다면, $q[C_{FK}]=t[C_i]$을 만족하는 $q\in Q_c$와 $t\in R_c$에 대하여,

① $q[TC]>t[TC]$이면, 연쇄 삭제 규칙과 널화 삭제 규칙만이 적용 가능하다.

② $q[TC]=t[TC]$이면, 모든 삭제 규칙이 적용 가능하다.

③ $q[TC]<t[TC]$이면, 제한 삭제 규칙만이 적용 가능하다.

모든 $u\in R_c$에 대하여, 비록 $t[A_i, C_i]=u[A_i, C_i]$이라도 $u[TC]<c$이면 ★-속성에 의하여 u를 삭제할 수 없다. 이 경우, t와 다중사례 요소인 u는 $R_{u[TC]}$와 $R_{c'>u[TC]}$에 계속 존재하게 된다. 따라서 다중사례 요소의 해석에 따른 갱신 의미를 완벽하게 지원하기 위해서는 다음을 추가하여야 한다.

- $t[A_i, C_i]=u[A_i, C_i]$이고 $u[TC]<c$인 $u\in R_c$가 존재하지 않는다.

3.5 선택 연산의 운영 의미

c-주체에 의한 선택 문장은 다음과 같은 형식을 지니게 된다.

```
SELECT  [* | Bi[, Bj]] ···
FROM    Rc
[WHERE  조건];
```

B_i는 데이타 혹은 분류 애트리뷰트가 될 수 있다. 선택 연산은 지정된 조건을 만족시키는 투플 $t \in R_i$의 지정된 필드 값을 선택한다. 그러나 단순 보안 속성에 의하여 $t[TC] \leq c$인 투플만이 선택되어야 한다. 다중사례가 존재하는 경우에, c-주체는 원하는 데이타를 선택할 수 있어야 한다.

3.6 다단계 갱신 연산의 분석

기존의 갱신 연산은 엔티티 무결성, 널 무결성, 인스턴스간 무결성, PI-FD 만을 유지하기 위한 관점에서 제한적으로 제안되었다. 이에 따라 다단계 참조 무결성 조건을 지원하지 못한다. 또한 다단계 처리 연산을 지원하지 못하며, 다중사례 요소의 해석에 따른 갱신 의미를 지원하지 못한다.

본 논문에서 제안된 다단계 릴레이션의 갱신 연산은 이러한 제한사항을 극복하며 다음과 같은 특징을 지닌다. 첫째, 다단계 데이타베이스를 일관된 상태로 유지하기 위하여 제안된 모든 다단계 무결성 제약조건을 지원한다. 둘째, 데이타에 대한 분류 값의 명시적인 지정을 주체에게 허용하므로써 단일 트랜잭션에 의한 다단계 처리를 지원한다. 셋째, 다단계 릴레이션의 갱신을 복잡하게 하는 다중사례를 허용하면서 이의 해석에 따른 다단계 릴레이션의 갱신을 지원한다.

4. 결 론

본 논문에서는 필드 수준에서의 다단계 보안을 지원하는 관계 데이타베이스 관리 시스템을 설계하기 위하여 관계 모델을 확장하고, 확장된 관계 모델을 위한 다단계 무결성 제약조건을 제시하며, 이에 따른 다단계 데이타베이스의 운영 의미를 제시한다.

다단계 보안을 위하여 확장된 관계 모델과 제안된 다단계 무결성 제약조건은 다단계 데이타베이스를 일관된 상태로 유지시키며, 다중사례를 지원하면서 이의 허용에 따른 엔티티 및 관계 표현의 모호성을 제거할 수 있는 기반을 제공한다.

확장된 다단계 릴레이션에 대한 다단계 갱신 연산은 모든 다단계 무결성 제약조건을 보장하며, 서로 다른 보안 분류의 요소를 동시에 처리할 수 있는 다단계 입력 및 갱신 트랜잭션을 지원하여 갱신 연산의 효율성을 증가시킨다.

참 고 문 헌

[1] R. Graubart, "Comparing DBMS and Operating System Security Requirements : The Need for a Separate DBMS Security Criteria," Proc. IFIP WG 11.3 Workshop on DB Sec. pp. 109-114, Sep. 1989.

[2] T. Y. Lin, "Bell and LaPadula Axioms : A "New" Paradigm for an "Old" Model," Proc. 1992-1993 ACM SIGSAC New Security Paradigms Workshop, pp. 82-93, 1993.

[3] D. E. Denning, T. F. Lunt, R. R. Schell, M. Heckman and W. Shockley, "A Multilevel Relational Data Model," Advances in Computer System Security, Vol. III, Artech House, Inc., pp. 234-248, 1988.

[4] T. F. Lunt, D. E. Denning, R. R. Schell, M. Heckman and W. Shockley, "The SeaView Security Model," IEEE Trans. SE., Vol. 16, No. 6, pp. 593-607, June 1990.

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

[6] R. Sandhu, S. Jajodia and T. Lunt, "A New Polyinstantiation Integrity Constraint for Multilevel Relations," Proc. Computer Security Foundations Workshop III, pp. 159-165, June 1990.

[7] S. Jajodia and R. Sandhu, "A Novel Decomposition of Multilevel Relations Into Single-Level Relations," Proc. 1991 IEEE Computer Society Symp. on Research in

Security and Privacy, pp. 300-313. May 1991.

[8] S. Jajodia and R. Sandhu, "Polyinstantiation Integrity in Multilevel Relations Revisited," Proc. IFIP WG 11.3 Workshop on DB Sec., pp. 297-307, Sep. 1990.

[9] R. Sandhu and S. Jajodia, "Referential Integrity in Multilevel Secure Databases," Proc. 16th Natl. Comp. Sec. Conf., pp. 39-52, Sep. 1993.

[10] V. M. Doshi and S. Jajodia, "Referential Integrity in Multilevel Secure Database Management Systems," Proc. IFIP/Sec '92, pp. 389-401, 1992.

[11] T. F. Lunt and D. Hsieh, "Update Semantics for a Multilevel Relational Database System," Proc. IFIP WG 11.3 Workshop on DB Sec., pp. 281-296, Sep. 1990.

[12] C. J. Date, Relational Database Selected Writings, Addison-Wesley, 1986.

[13] 조완수, "다단계 보안을 위한 관계 데이타 모델의 확장," 통신정보보호학회 논문지 제5권 제3호, 1995. 9.

조 완 수

1984년 인하대학교 전자계산학과(이학사)
1986년 미국 Univ. of Southwestern Louisiana 대학원 전자계산학과(전산학석사)
1991년~현재 인하대학교 대학원 전자계산학과 박사과정
1986년~현재 국방정보체계연구소 선임연구원
관심분야 : 데이타베이스, 컴퓨터 보안

배 해 영

1976년 인하대학교 응용물리학과(공학사)
1986년 연세대학교 대학원 전자계산학과(공학석사)
1990년 숭실대학교 대학원 전자계산학과(공학박사)
1985년 Univ. of Houston 객원교수
1982년~84년 인하대학교 전자계산소 소장
1982년~현재 인하대학교 전자계산공학과 교수
관심분야 : 데이타베이스(특히, 멀티미디어 데이타베이스 시스템, 실시간 데이타베이스 시스템, 지리 데이타베이스 시스템)