다단계 보안 관계형 데이타 모델을 위한 확장된 참조 무결성 의미론

(Semantics of an Extended Referential Integrity for Multilevel Secure Relational Data Model)

이 상 원 † 김 용 한 †† 김 형 주 †††

(Sang Won Lee) (Young Han Kim) (Hyung Joo Kim)

요 약 본 논문에서는 다단계 보안 관계형 데이타모델을 위한 확장된 참조 무결성 의미론 MLS-RIS(Multi Level Secure Referential Integrity Semantics)을 제안한다. 이 MLS-RIS는 단일 릴레이션을 위한 기존의 다단계 보안 관계형 데이타모델과 SQL 표준의 참조 무결성 의미론에 기반한다. 우선 두 다단계 릴레이션 사이의 참조 무결성을 정의하고, 다중 인스턴스화에 따른 참조 모호성의 해결규칙을 제안했다. 그리고, 이 프레임워크내에서 다단계 릴레이션에 삽입, 삭제 및 갱신 연산들에 대해 참조 무결성의 유지를 위한 동적 의미론을 정의하였다. MLS-RIS는 다음의 두가지 특징을 갖는다 - (1) 다단계 보안 관계형 데이타모델에서 발생하는 참조 모호성의 문제를 해결 규칙을 통해 해결하고자 했고, (2) SQL 표준의 외래키 명세에 기반하여 참조 무결성의 동적 의미론을 최초로 정의했다.

Abstract In this paper, we propose the semantics of an extended referential integrity for multilevel secure relational data model, called MLS-RIS(Multi Level Secure Referential Integrity Semantics). This MLS-RIS is based on both the traditional multilevel secure relational data model for single relation and the semantics of SQL standard referential integrity. First, we define the referential integrity to be held between two multilevel relations, and propose a rule to resolve the referential ambiguities which are due to the poly-instantiation phenomena of the multilevel secure data model. And within this framework, we define the dynamic referential semantics of the SQL update operations, including insert, delete, and update, in order to preserve the referential integrity. The uniqueness of the MLS-RIS is two-fold: (1) it tries to solve the referential ambiguity problems in multilevel secure relational data model, by introducing a resolution rule, and (2) to the best of our knowledge, there is no work on the dynamic semantics of referential integrity in multilevel secure relational data model, except for our MLS-RIS.

1. 서 론

데이타베이스는 여러명의 사용자가 접근하기 때문에, 정보의 보안을 위해서 DBMS는 정보에 대해 정당한 자격이 있는 사용자만이 정보를 접근하도록 하는 접근제어 장치를 반드시 갖추고 있어야 한다. 접근제어 장치의 기능은 다음과 같은 추상적인 모델로 표시할수 있다.

$$F(S,O,T) = \text{yes or no}$$

여기서 S, O, T는 각각 사용자, 데이타, 접근 형식(읽기, 쓰기, 변경 등)을 나타낸다 함수 F로 표시되는 접근제어 장치의 기능은 사용자 S가 데이타 O에 대해 T형식의 접근을 요청할때, 이의 허용여부를 결정하는 것이다.

데이타베이스 시스템의 접근제어 모델은 크게 임의적

· 본 연구는 과학기술처 지원 과제 "웹 트랜잭션 서버를 위한 객체지향 콤포넌트 기술개발"의 일부 지원에 의한 것임.

† 학생회원 : 서울대학교 컴퓨터공학과
swlee@candy snu ac.kr
†† 비 회 원 : 한국오라클
kimyh@kr oracle.kr
††† 종신회원 : 서울대학교 컴퓨터공학과 교수
hjk@oopsla san ac kr

논문접수 : 1997년 10월 21일
심사완료 : 1998년 3월 31일

접근제어(discretionary access control)와 강제적 접근제어(mandatory access control)로 분류할 수 있다. 임의적 접근제어는 함수 F의 값의 결정을 사용자의 권한을 표시한 자료구조, 예를 들어 접근 행렬이나 접근제어 리스트 등을 참조하여 결정한다. 반면에 강제적 접근제어는 사용자와 데이타 각각에 부여된 보안등급을 기반으로 하여 사용자의 접근을 제어한다. 강제적 접근제어는 사용자와 데이타에 부여할 수 있는 보안등급이 여러 개가 있다는 의미에서 다단계 보안(multilevel security)이라고도 한다. 이 글에서는 강제적 접근제어라는 용어 대신 다단계 보안이라는 용어를 사용하겠다. 특히 다단계 보안 모델은 최근 들어서 실시간 데이타베이스[8, 12,25] 등의 영역에서 많은 주목을 받고 있다.

현재의 대부분의 관계형 DBMS에서는 릴레이션(relation), 뷰(view), 속성(attribute) 단위까지의 임의적 접근제어를 지원하고 있다. 관계형 DBMS에서 취하고 있는 이 동적 권한 관리 방법은 [10]에 자세히 설명되어 있다 관계형 데이타모델을 확장하여 다단계보안을 지원하는 대표적인 연구로서는 SeaView 모델 [21], LDV 모델 [26], Jajodia-Sandhu 모델 [16,18] 등이 있다. 데이타베이스의 응용의 범위가 은행, 행정업무에서 CAD, A.I, Multimedia의 영역으로 확대되면서 기존 관계형 DBMS는 새로운 응용의 환경에서 요구되는 성능이나 모델링 능력면에서 부적당하다 [3]. 이러한 단점을 극복하기 위해서 관계형 데이타모델을 확장하거나, 복합 객체, 여러가지 의미상의 관계, 임의의 자료형 정의를 가능하게 해주는 객체지향 데이타모델이 나왔는데, 이 중의 하나인 ORION에서는 임의적 접근제어를 지원하고 있으며 [23], 강제적 접근제어 모델로는 ORION을 확장한 SORION 모델 [27], 버전 개념을 이용해서 다중인스턴스화를 효과적으로 지원하는 MORION 모델 [1] 등이 있다. 표 1은 위에서 설명한 데이타베이스의 접근제어 상황을 분류한 것이다.

표 1 데이타베이스 접근제어 분류

	RDBMS	OODBMS
임의적 접근제어	대부분의 DBMS들	ORION
다단계 보안 모델	SeaView, LDV, Jajodia-Sandhu	SORION, MORION

기존의 다단계 관계형 데이타 모델에 관한 연구는 주로 단일 릴레이션(relation)에 국한되었고, 둘 이상의 릴레이션의 투플(tuple)들간의 참조 관계에 관한 연구는 별로 없었다. 즉, 관계형 데이타모델의 핵심 요소중의 하나인 참조 무결성(referential integrity)을 고려한 다단계 보안 모델에 관한 연구가 부족했다. 이러한 사실에 기반하여, 본 논문에서는 관계형 데이타베이스 표준인 SQL에서의 참조 무결성 의미론(referential integrity semantics)을 다단계 보안 모델을 위해 확장한 **MLS-RIS**(*M*ulti *L*evel *S*ecure *R*eferential *I*ntegrity *S*emantics)를 제안한다.

1.1 논문의 구성

우선 2장에서는, 논문의 전개에 필요한 범위내에서, **MLS-RIS**와 관련한 기본 개념들 - 즉, 단일 릴레이션에 대한 다단계 관계형 데이타 모델과 표준 관계형 데이타모델에 있어서의 참조 무결성 - 에 관해 설명한다. 3장에서는 2장의 개념들을 기반으로 **MLS-RIS**의 참조 무결성을 정의하고, 이때 발생하는 참조 모호성(referential ambiguity)과 그의 해결 방안을 제시한다. 또한, 이 참조 무결성과 참조 모호성의 개념에 기반하여, 다단계 보안 관계형 데이타모델의 릴레이션에 대한 삽입, 삭제, 갱신 등의 연산의 동적인 참조 의미론을 기술한다. 4장에서 관련연구와 **MLS-RIS**의 차이점을 설명하고 5장에서 결론을 맺는다.

2. 기본 개념

2.1 다단계보안 모델

다단계보안 모델에서는 모든 데이타와 사용자에게 보안등급(security level)을 부여한다. 대표적인 다단계보안 모델로는 Bell-LaPadula 모델 [4] 을 들 수가 있는데, 이는 데이타의 보안을 위해, 사용자가 데이타를 접근할 때 다음 두가지의 중요한 성질을 반드시 만족해야 한다.

1. 단순 보안 성질: 사용자 s는 데이타 o에 대해, $L(o) \le L(s)$일때만 읽기접근을 할 수있다.

$$F(s, o, R) = yes \text{ iff } L(s) \ge L(o)$$

2. *-성질: 사용자 s는 다른 데이타 o에 대해, $L(s) \le L(o)$일 때만 쓰기접근을 할수 있다.

$$F(s, o, W) = yes \text{ iff } L(s) \ge L(o)$$

첫번째 성질은 사용자보다 높은 보안등급을 가진 데이타에 대한 접근을 방지하기 위한 것이다. 두번째 성질은 그림 1과 같이, 높은 보안등급을 가진 객체의 내용이 낮은 보안등급의 객체에 옮기므로서 일어나는 잘못된 정보 흐름을 방지하기 위한 것이다. 본 논문에서는 사용자와 데이타에 대해 순차적인 보안 등급 *U*(*un*-

classified) ≤ *C(confidential)* ≤ *S(secret)* ≤ *TS (top-secret)*을 가정한다. 기호 < 나 ≤등은 사용자나 데이타에 부여된 보안등급들사이의 비교를 위한 연산자이다.

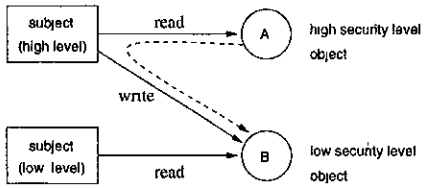

그림 1 잘못된 정보흐름의 예

2.2 다단계 관계형 데이타 모델: 다단계 릴레이션

다단계 릴레이션 R의 스키마는 다음과 같이 각 데이타 속성 A_i와 그의 보안등급 속성 C_i, 그리고 하나의 투플 전체의 보안등급 속성 TC로 이루어진다 [9,16].

$$R(A_1, C_1, \ldots, A_n, C_n, TC)$$

다단계 릴레이션 R의 한 투플은 다음과 같이 표시된다.

$$(a_1, c_1, \ldots, a_n, c_n, tc)$$

[9,16] 등에서는 다단계 릴레이션의 투플 t에 대해 다음의 몇가지 무결성 성질을 가정하고 있다. 첫째, 투플 t의 주키(primary key) 값 t_{PK}는 표준 관계형 데이타 모델과 마찬가지로 *null* 값을 가질 수 없다. 둘째, 하나 이상의 속성으로 이루어진 주키의 경우 투플 t의 주키의 각 속성의 보안 등급은 균일하다. 세째, 주키를 제외한 속성의 보안등급은 주키의 보안등급보다 높거나 같다 마지막으로, 투플 보안 등급은 속성 보안 등급의 lub(least upper bound)이다. 본 논문에서는 설명의 편의를 위해 하나의 속성으로 이루어진 주키를 가정하겠다.

그림 2는 본 논문에서 설명을 위해 계속 사용할 다단계 릴레이션 *SMD*의 한 예을 보여주고 있다. 그런데, 그림 2는 보안등급 *TS*을 가진 사용자에게 보여지는 내용이다. Bell-LaPadula 모델의 단순 보안성질에 따라, 사용자의 보안등급에 따라 보여지는 릴레이션의 내용이 달라진다. 따라서, 하나의 다단계 릴레이션 R에 대해 각 보안등급 C에 해당하는 **릴레이션 인스턴스** R_c가 존재하게 된다. 예를 들어, 그림 3은 C 보안등급을 갖는 사용자에게 보여지는, 그림 2의 *SMD*의 릴레이션 인스턴스 SMD_C를 보여주고 있다[1]. 그림 3에서 투플 보안등급이 C보다 큰 투플들은 사용자에게 보여지지 않음을 알수 있다 그림 2는 SMD_{TS}와 동일하다.

릴레이션 *SMD*

SHIP		MISSION		DEST		TC
Apollo	U	탐사	U	달	U	U
Pathfinder	C	탐사	C	화성	C	C
Pathfinder	C	핵실험	S	화성	C	S
Cassini	TS	탐사	TS	토성	TS	TS

그림 2 다단계 릴레이션의 예

SHIP		MISSION		DEST		TC
Apollo	U	탐사	U	달	U	U
Pathfinder	C	탐사	C	화성	C	C

그림 3 다단계 릴레이션 *SMD*의 *C*-레벨의 인스턴스 SMD_C

2.2.1 다중인스턴스화와 관계형 데이타 모델

다중인스턴스화(polyinstantiation)란, 다단계 보안 모델에서 데이타를 취급할 때 데이타의 값은 같으면서 보안등급을 달리하는 여러개의 데이타가 동시에 존재하는 것을 일컫는다. 다단계 데이타를 취급할때 다중인스턴스화는 불가피한 현상이다 [20]. 즉, 다중인스턴스화는 높은 보안등급의 사용자가, 낮은 보안등급의 사용자에게 정보의 유출을 막으면서, 자신의 보안등급상에서 따로 필요로 하는 정보를 유지하기 위해 필요하다. 달리 해석하면, 다중인스턴스화는 Bell-LaPadula 모델의 *-성질을 만족시키기 위해서이기도 하다.

다단계 관계형 데이타모델에서 발생하는 다중인스턴스화의 종류는 다중인스턴스화된 개체와 다중인스턴스화된 속성의 두가지로 나눌수 있다. 다중인스턴스화된 개체는, 같은 주키의 값을 서로 다른 보안등급상에서 각기 필요로 하는 경우이다. 예를 들어, 주키의 값을 이미 높은 보안등급의 사용자가 어떤 개체의 값으로 할당한 뒤에, 낮은 보안등급의 사용자가 그 값을 자신이 새로 생성하는 투플의 주키로 사용하고자 할 때 발생한다. 만일 이때 같은 주키 값이 존재한다는 이유로 투플의 생

1) 이때 실제로 각 보안등급에 해당하는 릴레이션들이 중복적으로 데이타베이스에 저장되는 것이 아니라, 특정 다단계 릴레이션의 내용은 [18] 등의 방법을 사용해서 여러개의 릴레이션에 분해되어 저장되었다가 특정 보안 등급에 맞게 복원되어져 보여진다.

성을 거부하는 경우 높은 C-레벨의 보안등급상의 개체의 존재가 낮은 보안등급의 사용자에게 유출되는 효과가 있다. 그림 4의 **Apollo**를 키값으로 갖는 두 투플이 다중인스턴스화된 개체를 모델링하고 있다. 이때는 실제로 이름은 같으나, 서로 별개의 두대의 우주선이 존재하는 경우이다. 다중인스턴스화된 속성은 하나의 개체의 특성을 묘사하는 속성의 값이 각 보안등급상에서 서로 틀린 경우이다. 예를 들어, 그림 3의 **Pathfinder**호를 표현하는 두 투플은 다중 인스턴스화된 속성을 모델링하고 있다. 하나의 **Pathfinder**호의 임무가 C-보안등급의 사용자에게는 단순한 탐사이지만, S-등급의 사용자에게는 핵실험일 경우를 표현하고 있다. 다중인스턴스화와 관련한 자세한 내용은 [17,20] 등을 참조하기 바란다.

SHIP		MISSION		DEST		TC
Apollo	U	탐사	U	달	U	U
Apollo	TS	탐사	TS	토성	TS	TS

그림 4 다중인스턴스화된 개체의 예

2.3 참조 무결성

참조 무결성은, 개체 무결성(entity integrity)과 더불어 관계형 데이타모델의 핵심요소로서, Codd [6], Date [7] 등에 의해 개념이 정립되어, 현재는 SQL2 [14], SQL3 [13] 등의 관계형 데이타베이스 표준에 포함되어 있다.

참조 무결성이란, 특정 릴레이션 R_P의 주키(primary key) $R_P.PK$와 이 주키를 참조하는 다른 릴레이션 R_C[2]의 외래키(foreign key)사이에 반드시 만족되어야 하는 조건으로, R_C의 임의의 투플 t의 $t[FK]$값은 널(*null*)값이거나 R_P에 같은 값을 주키로 갖는 투플이 반드시 존재해야 한다.

참조무결성 1 SQL 표준에서의 참조 무결성 $t \in R_C$, $t[FK] \neq null$인 투플 t에 대해, R_P에는 $t[FK] = q[PK]$ 하나의 투플 q가 반드시 존재해야 한다.

다음은 SQL3 [13] 에서 참조 무결성의 선언과 관련한 구문을 보여주고 있는데, 데이타 정의어(data definition language)를 이용해서 R_C의 선언시에 추가적으로 외래키와 참조 무결성의 동적 의미론을 정의하는데 사용된다.

```
FOREIGN KEY [(<referencing columns>)]
   REFERENCES [PENDANT] <table name> [(<refer-
   enced columns>)]
   [MATCH FULL | MATCH PARTIAL]
   [ON UPDATE { CASCADE | SET NULL | SET
   DEFAULT | RESTRICT | NO ACTION }]
   [ON DELETE { CASCADE | SET NULL | SET
   DEFAULT | RESTRICT | NO ACTION }]
```

위의 구문에서 **<referencing columns>**은 R_C의 외래키 $R_C.FK$를, **<table name>**은 참조되는 R_P를 나타낸다. SQL92에서는 **<referenced columns>**에 R_P의 후보키 (candidate key)도 지정할 수 있으나, 본 논문에서는 항상 주키로 가정한다. 마지막 두 줄은 R_P에서 특정 투플 t의 주키의 값 $t[PK]$가 변경되거나 t가 삭제될 때, R_C에서 이를 참조하고 있는 투플들을 어떻게 처리할 것이가를 명시하는데 사용된다. 예를 들어, R_P의 한 투플 t가 삭제될 때, **CASCADE**는 참조 무결성 조건을 만족시키기 위해 R_C에서 $t'[FK] = t[PF]$인 모든 투플을 삭제한다. **SET NULL**의 경우 $t[PK]$값을 참조했던 모든 투플들의 외래키 값을 모두 *null*로 세팅하게 된다. **RESTRICT** 명세는 만일에 R_P의 특정 투플 t를 삭제하거나 주키 값을 변경하고 하는 경우에, R_C의 임의의 투플이 t를 참조하고 있는 경우 해당 연산을 금지하는 것이다.

릴레이션 *CS*

CAPTAIN	SHIP
Clinton	Pathfinder

릴레이션 *SMD*

SHIP	MISSION	DEST
Pathfinder	탐사	화성

(a) 튜플 (Pathfinder,탐사, 화성) 삭제전

CAPTAIN	SHIP

SHIP	MISSION	DEST

(b) 삭제 후

그림 5 참조 무결성의 연쇄삭제(CASCADE DELETE)

SET DEFAULT, NO ACTION과 관련해서는 본 논문에서는 다루지 않겠다. **SET DEFAULT**의 경우 R_P의 투플의 삭제나 갱신의 경우 참조하는 투플의 외래키 값을 외래키 선언시에 지정한 특정 값으로 세팅한다. **NO ACTION**의 경우 R_P의 투플값을 변경하는 트랜잭션의 종료 (commit) 시에 참조 무결성 조건을 검사한

2) R_P와 R_C는 각각 부모 릴레이션(parent relation), 자식 릴레이션(child relation)을 나타낸다.

다. 이들과 **PENDANT, MATCH** 키워드와 관련된 의미는 논문의 논의에서 제외한다. 자세한 내용은 [13] 을 참조하기 바란다.

표 2는 본 논문에서 다루고자 하는 참조 무결성 의미론의 범위를 보여주고 있다. 즉, 세 가지의 참조 무결성 관련 동작 **CASCADE, RESTRICT, SET NULL**과, R_P 및 R_C에 대한 삽입, 삭제, 그리고 갱신 연산의 조합을 보여주고 있다. 그림에서 o로 표시된 조합의 경우 참조 무결성이 항상 만족시킨다. 예를 들어, R_P에 새로운 투플의 삽입하는 연산의 경우 참조 무결성을 위반하지 않는다. - 표시된 조합의 경우 해당 연산에 의해 영향을 받는 투플의 외래키 값이 R_P에 존재하는지 참조 무결성 조건을 검사해야 한다. 마지막으로,

? 표시가 된 조합의 경우는 앞에서 설명한 바와 같이 참조 무결성을 만족시키기 위해 의미을 정의한 경우이다.

표 2 SQL2에서의 참조 무결성 지원

	R_P			R_C		
	삽입	삭제	갱신	삽입	삭제	갱신
CASCADE	o	?	?	-	o	-
RESTRICT	o	?	?	-	o	-
SETNULL	o	?	?	-	o	-

o = 항상 참조무결성을 만족시킴
- = 참조무결성 검사
? = 참조무결성의 동적 의미론

3. MLS-RIS

이 장에서는 **MLS-RIS**에서의 참조 무결성의 정의, 참조 모호성의 해결규칙을 우선 설명하고, 이를 기반으로 참조 무결성의 유지를 위한 SQL의 삽입, 삭제, 변경 연산들의 동적 의미론을 외래키 명세조건 **CASCADE, RESTRICT, NULL** 각각에 대해 설명한다.

3.1 다단계 보안 관계형 데이타모델의 참조 무결성 (MLS-RIS)

다음 참조 무결성 성질 2는, 참조관계에 있는 두 다단계 릴레이션 R_P와 R_C사이에 성립해야 하는 **MLS-RIS**의 외래키 무결성 성질이다.

참조무결성 2 MLS-RIS 참조 무결성 성질 $t \in R_C$, $t[FK] \neq null$인 모든 t에 대해, 다음의 조건을 만족하는 어떤 투플 $q \in R_P$가 반드시 존재해야 한다.

1. $t[FK] = q[PK]$
2. $t[C_{FK}] \geq q[C_{PK}]$
3. $t[C_{FK}] \geq q[TC]$

첫번째 조건은 표준 관계형 데이타모델의 참조 무결성과 같은 의미이다. 두번째 조건은 외래키 값의 보안등급은 해당 투플의 주키의 보안등급과 동일하거나 커야 한다는 것이다 이는 Bell-LaPadula모델의 단순 보안 성질을 만족시키기 위한 것이다. 세번째 조건은 R_P의 해당 투플 q는 $t[C_{FK}]$를 접근가능한 사용자에게 보이는 투플이어야 함을 의미한다.

그런데, 다단계 보안 관계형 데이타 모델의 다중인스턴스화된 개체와 다중인스턴스화된 속성은 참조 무결성과 관련하여 참조 모호성 문제를 야기한다 [11]. 예를 들어, 그림 6에서 R_C (릴레이션 *CS*)에서 참조하는 **Pathfinder**호는 R_P (릴레이션 *SMD*) 의 세 투플중 어떤 투플을 가리키는지 애매하다. 즉, **Clinton**은 다중인스턴스화된 개체 관계에 있는 *C*-레벨과 *S*-레벨의 두 **Pathfinder**호중 어느 우주선의 선장인지, 또는 다중인스턴스화된 속성 관계에 있는 *C*-레벨의 두 투플중의 어느 것을 참조하는지가 애매하다. 이때 우리 '투플 **(Clinton, Pathfinder)**의 참조키는 "참조 모호성"을 갖는다'라고 한다. 그리고, 그림 6의 R_P의 세 투플은 '투플 **(Clinton, Pathfinder)**의 참조키에 대해 참조 모호성을 유발시킨다'라고 한다. 이와 같은 참조 모호성은 다단계 관계 데이타모델에서 참조 무결성을 지원하기 위해서는 반드시 해결해야 한다.

CAPTAIN		SHIP		TC
Clinton	S	Pathfinder	S	S

(a) R_C: 릴레이션 *CS*

SHIP		MISSION		DEST		TC
Pathfinder	C	탐사	C	화성	C	C
Pathfinder	C	핵실험	S	화성	U	S
Pathfinder	S	탐사	S	태양	S	S

(b) R_P: 릴레이션 *SMD*

그림 6 다단계 관계형 데이타 모델의 참조 모호성

3.2 참조 모호성의 해결 규칙

이 절에서는 앞에서 지적한 참조 모호성과 관련한 **MLS-RIS**의 해결방안을 설명하고자 한다. 먼저 다음에

나와 있는 MLS-RIS의 참조 모호성의 해결규칙을 보자.

참조무결성 3 참조 모호성의 해결 규칙(resolution rules
참조 모호성을 갖는 R_C의 임의의 투플 $t[FK]$에 대해 참조 모호성을 유발시키는 투플 t''들에 대해,

1. $t[FK]$는 $t''[C_{PK}]$가 가장 높은 투플을 참조한다.
2. 1.의 조건에 해당하는 투플이 하나 이상일 때는, $t[FK]$는 $t''[TC]$가 가장 높은 투플을 참조한다.

첫번째 규칙은 다중인스턴스화된 개체 관계에 있는 하나 이상의 투플들중에서 가장 높은 보안등급의 주키를 갖는 투플을 참조한다는 의미이고, 두번째 규칙은 다중인스턴스화된 속성 관계의 투플들중에서 가장 상위보안등급의 투플을 참조하도록 지정하고 있다. 위 MLS-RIS 참조 모호성 해결 규칙은 다단계 보안 모델에서 발생하는 참조 모호성은 전적으로 사용자의 책임이라는 원칙에 기반한다. 즉, 특정 보안 등급의 사용자는 자신이 접근하는 릴레이션 인스턴스에서 생기는 모든 참조 모호성과 관련한 현상을 인식해야 하고 올바른 참조 관계의 유지에 대한 관리를 자신이 직접해야 한다. 예를 들어, 그림 6의 릴레이션 R_P에서 사용자가 투플 (Pathfinder,S,탐사,S,태양,S,S)을 삭제하는 경우, 그림 7에서 보여지듯이 투플 (Clinton,Pathfinder)에서 참조하는 투플이 (Pathfinder,C,핵실험,S,화성,U,S)로 바뀜을 알아야 한다. 반대로, 사용자가 그림 7의 R_P에 투플 (Pathfinder,S,탐사,S,태양,S,S)을 삽입하는 경우, 투플 (Clinton,Pathfinder)는 새로 삽입된 투플을 참조하게 된다.

CAPTAIN		SHIP		TC
Clinton	S	Pathfinder	S	S

(a) R_C

SHIP		MISSION		DEST		TC
Pathfinder	C	탐사	C	화성	C	C
Pathfinder	C	핵실험	S	화성	U	S

(b) R_P

그림 7 다중인스턴스화된 개체 투플의 삭제에 따른 참조관계의 의미적 변화

3.3 MLS-RIS의 동적 의미론

이 절에서는 앞에서 기술한 MLS-RIS의 참조 무결성과 참조 모호성 해결 규칙에 기반하여 MLS-RIS의 참조 무결성과 관련한 동적 의미론을 기술하고자 한다. 이들 동적 의미론의 설명은 2장의 표 2의 구분에 따른다.

3.3.1 R_C의 투플 삽입, 갱신, 삭제

SQL 표준에서, 표 2에 나와 있듯이, R_C 투플의 삽입 및 갱신의 경우에는 참조 무결성의 만족 여부를 검사해야 한다. 이는 MLS-RIS에도 마찬가지로 해당한다

MLS-RIS 규칙 1 R_C에 투플 t의 삽입(갱신) R_C에 새로 삽입되는(갱신되는) $t[FK] \neq null$인 투플 t에 대해, R_P에는 $t'[PK] = t[FK]$이고 $t'[C_{PK}] \leq t[C_{FK}]$인 투플 t'가 반드시 존재해야 한다. 만일 그렇지 않은 경우에는 투플 t의 삽입(갱신)은 실패한다.

이때, 위의 조건을 만족하는 투플 t'가 하나 이상인 경우, t는 의미적으로 $t'[TC] \leq t[C_{FK}]$인 투플들 중에서 가장 높은 보안등급을 갖는 투플을 가리킨다. R_C의 투플의 삭제의 경우는, SQL 표준의 경우와 마찬가지로, 항상 MLS-RIS 참조 무결성을 만족하기 때문에 어떤 검사도 필요하지 않다.

3.3.2 R_P의 삽입의 의미론과 참조 관계의 변화

SQL 표준에 있어서 R_P에 새로운 투플의 삽입은 참조 무결성과 관련하여, 어떤 영향도 미치지 않는다. 그러나, MLS-RIS에 있어서는 새로운 투플 t의 삽입은, 앞에서 언급한 바와 같이, 다중인스턴스화된 개체 관계에 의한 참조 모호성의 해결원칙에 의해 다음과 같은 의미적인 변화가 생긴다.

MLS-RIS 규칙 2 R_P에 투플 t의 삽입 R_P에 $t'[PK] = t[PK]$이고 $t'[C_{PK}] \leq t[C_{PK}]$인 어떤 투플 t'가 이미 존재하는 경우(즉, 다중인스턴스화된 개체 관계에 있는 하위등급의 투플이 있는 경우), $t''[FK] = t[PK]$이고, $t''[C_{FK}] \geq t[C_{PK}]$인 R_C의 모든 투플들은 의미적으로 새로운 투플 t를 참조하게 된다. 투플 t'가 존재하지 않는 경우, 참조 관계에 있어 아무런 영향을 미치지 않는다.

앞절에서 예로 들었듯이, 사용자가 그림 7의 R_P에 투플 (Pathfinder,S,탐사,S,태양,S,S)을 삽입하는 경우, R_C의 투플 (Clinton,Pathfinder)는 새로 삽입된 투플을 참조하게 된다. 위의 조건을 만족하는 투플 t'가 존재하지 않는 경우는, 투플 t의 삽입 이전에 $t[PK]$값을 외래키로 갖는 $t''[FK]$가 R_C에 존재하지 않기 때문에 참조관계에 아무런 영향을 미치지 않는다.

3.3.3. R_P의 투플 삭제의 의미론

다음의 세가지 MLS-RIS 의미론은 R_P에 존재하는 투플을 삭제할 때, 외래키 선언 사양인 CASCADE,

RESTRICT, SET NULL 각각의 경우에 해당하는 의미적 변화이다.

MLS-RIS 규칙 3 R_P에 투플 t의 삭제 (CASCADE) t의 삭제시 R_P에 $t'[PK] = t[PK]$이고 $t'[C_{PK}] \leq t[C_{PK}]$이고 $t'[TC] \leq t[TC]$인 어떤 투플 t'가 존재하는 경우 (즉, 다중인스턴스화된 개체나 다중인스턴스화된 속성 관계에 있는 하위등급의 투플이 있는 경우), $t''[FK] = t[PK]$이고, $t''[C_{FK}] \geq t[C_{PK}]$인 R_C의 모든 투플들은 의미적으로 t'들중에서 $t'[C_{PK}]$가 가장 높은 투플을 가리키게 된다. 위의 투플 t'가 존재하지 않는 경우, 모든 t''는 R_C에서 삭제된다

CAPTAIN		SHIP		TC
Clinton	S	Pathfinder	S	S

(a) R_C

SHIP		MISSION	DEST	TC
Pathfinder	C	탐사 C	화성 C	C

(b) R_P

그림 8 R_P의 투플 삭제에 따른 연쇄삭제의 의미

예를 들어, 그림 7의 R_P에서 투플 **(Pathfinder, 핵실험, 화성)**이 삭제되는 경우, 의미적으로 이 투플을 참조하던 R_C의 투플 **(Clinton, Pathfinder)**는 연쇄삭제되는 대신에 그림 8에서 보여지듯이 의미적으로 투플 **(Pathfinder, 탐사, 화성)**를 가리키게 된다. 만일 S 보안등급의 사용자가 다음의 질의를 수행하게 된다면, **(Pathfinder, 핵실험, 화성)**의 삭제 이전과 삭제 후의 결과는 각각 **(핵실험)**과 **(탐사)**가 된다.

```
Select MISSION
from SMD, CS
where CAPTAIN = 'Clinton';
```

그리고, 그림 8에서 투플 **(Pathfinder, 탐사, 화성)**가 최종적으로 삭제될 때, R_C의 투플 **(Clinton, Pathfinder)**도 따라 삭제된다.

MLS-RIS 규칙 4 R_P에 투플 t의 삭제 (RESTRICT) t의 삭제시 R_P에 $t'[PK] = t[PK]$이고 $t'[C_{PK}] \leq t[C_{PK}]$이고 $t'[TC] \leq t[TC]$인 어떤 투플 t'가 존재하는 경우, CASCADE의 경우와 동일하다. 투플 t'가 존재하지 않고 t''가 하나 이상 존재하는 경우, t의 삭제는 실패한다.

MLS-RIS 규칙 5 R_P에 투플 t의 삭제(SET NULL) t의 삭제시 R_P에 $t'[PK] = t[PK]$이고 $t'[C_{PK}] \leq t[C_{PK}]$이고 $t'[TC] \leq t[TC]$인 어떤 투플 t'가 존재하는 경우, CASCADE, RESTRICT의 경우와 동일하다. 투플 t'가 존재하지 않고 t''가 하나 이상 존재하는 경우, $t''[FK]$의 값은 *null*로 바뀐다.

위의 두 규칙에서 보여지듯이, RESTRICT와 SET NULL의 경우에도, R_P에서 삭제되는 투플 t와 다중인스턴스화 관계의 하위 투플 t'가 존재할 때, R_C의 투플들은 t'로 의미적인 참조관계를 변화시킨다.

3.3.4 R_P의 주키값 갱신의 의미론

본 절에서는 R_P의 투플 t의 주키 값의 변경 이전 값을 $t[PK_{old}]$, 새로운 주키 값을 $t[P_{new}]$로 표시한다.

MLS-RIS 규칙 6 R_P에 투플 t의 주키 값 변경 (CASCADE) R_C에 $t'[FK] = t[PK_{old}]$이고 $t'[C_{FK}] \geq t[C_{PK}]$인 어떤 투플 t'가 존재하는 경우, $t'[FK]$는 값이 $t[PK_{new}]$로 바뀐다.

R_C에서 $t''[FK] = t[PKold]$이고 $t''[C_{FK}] \leq t[C_{PK}]$인 투플들 t''의 경우는 아무런 영향을 받지 않는다. 왜냐하면, 이들은 의미적으로 투플 t'를 참조하지 않고, 대신에 t'와 다중인스턴스화된 속성 관계에 있는 하위등급의 투플을 참조하고 있기 때문이다. RESTRICT와 SET NULL의 경우에도, 다음의 두 규칙에서 보여지듯이, CASCADE와 유사하다.

MLS-RIS 규칙 7 R_P에 투플 t의 주키 값 변경 (RESTRICT) R_C에 $t'[FK] = t[PK_{old}]$이고 $t'[C_{FK}] \geq t[C_{PK}]$인 어떤 투플 t'가 존재하는 경우, $t'[FK]$의 변경은 허용하지 않는다.

MLS-RIS 규칙 8 R_P에 투플 t의 주키 값 변경 (SET NULL) R_C에 $t'[FK] = t[PK_{old}]$이고 $t'[C_{FK}] \geq t[C_{PK}]$인 어떤 투플 t'가 존재하는 경우, $t'[FK]$의 값은 *null*로 바뀐다.

4. 관련 연구

다단계 관계형 데이타 모델에서의 참조 무결성에 관한 기존 연구로는, 놀랍게도 SeaView 모델 [9,21] 과 Sandhu-Jajodia 모델 [24] 만을 들 수 있다. 그리고, 이들 연구에 있어서도 참조 무결성의 성질만을 정의했을 뿐, 동적 의미론에 관한 언급은 없다. 이 장에서는 이 연구들에서 제시한 참조 무결성의 의미와 문제점을 살펴보고, 이들과 MLS-RIS와의 차이점을 설명하겠다.

Denning 등은 [9]에서 SeaView 모델을 제안하면서 다단계 관계형 데이타 모델에서의 참조 무결성에 대해 최초로 언급하였다. 다음은 [9] 에서 제안된 SeaView

모델의 참조 무결성 성질이다.

참조무결성 4 SeaView 1 $t \in R_C$, $t[FK] \neq null$인 모든 t에 대해, R_P에는 $q[FK] = t[FK]$이고 $q[C_{PK}] \leq t[C_{FK}]$인 투플 q가 반드시 존재해야 한다.

이 방법은 3장에서 언급한 참조 모호성의 문제를 안고 있다. Lunt [21] 등은 이 참조 모호성 문제를, 해결 규칙을 통해 극복하는 **MLS-RIS**와는 달리, 다음과 같이 참조 무결성의 의미를 좀 더 제한하므로써 해결하고자 했다.

참조무결성 5 ScaView 2 $t \in R_C$, $t[FK] \neq null$인 모든 t에 대해, R_P에는 $q[FK] = t[FK]$이고 $q[C_{PK}] = t[C_{FK}]$인 투플 q가 반드시 존재해야 한다

그러나, 이 참조 무결성 의미는 참조 모호성의 문제는 피하나, [24]에서 지적한 것처럼, 다단계 관계형 데이타모델의 모델링 능력(modelling power)을 제한하는 단점이 있다. 예를 들어, 그림 6에서 R_C에 투플 **(Clinton, S, Pathfinder, S, S)**은 R_P에 투플 **(Pathfinder, S, 탐사, S, 태양, S, S)**이 존재하기 때문에 참조 무결성을 만족시키나, 그림 7의 경우는 참조 무결성을 위배한다.

Sandhu 등은 이와 같은 문제점을 동시에 해결하기 위해, 다단계 관계형 데이타베이스의 설계 단계에서 다중인스턴스화된 개체 관계의 발생을 배제한 상태에서[3], 다음과 같은 참조 무결성 성질을 제안했다.

참조무결성 5 *Sandhu-Jajodia* $t \in R_C$, $t[FK] \neq null$인 모든 t에 대해, R_P에는 $q[FK] = t[FK]$이고 $q[C_{PK}] \leq t[C_{FK}]$이고 $q[TC] \leq t[C_{FK}]$인 투플 q가 반드시 존재해야 한다.

Sandhu-Jajodia의 참조 무결성의 정의는 **MLS-RIS**의 참조 무결성과 동일하다. 그러나, Sandhu-Jadodia 모델은 다중인스턴스화된 개체 관계에 있는 투플들에 의한 참조 모호성의 문제는 여전히 남아있다. 그리고, 다중인스턴스화된 속성 관계의 배제로 의한 모델링 능력의 저하도 이 모델의 단점이다.

3) 예를 들어, 릴레이션의 정의시에 각 보안 등급상에서 주키로 사용할 수 범위를 구분한다. 따라서, 그림 6의 R_C에서와 같이, 주키의 값은 같으나 보안등급을 달리하는 투플이 두개 이상 존재할 수 없다.

본 논문에서 제안한 **MLS-RIS**는 SeaView 모델이나 Sandhu-Jajodia 모델과 비교해서 다음과 같은 특징들을 갖는다. 첫째, 다단계 관계형 데이타 모델의 참조 무결성과 관련하여 SQL 표준에서 지원하는 참조 무결성의 동적 의미론을 확장해서 정의했다. 둘째, 참조 모호성 해결 규칙을 도입해서 다중인스턴스화된 개체나 다중인스턴스화된 속성 관계에 있는 투플들에 의한 참조 모호성 문제를 해결하고자 했다. 물론 이 방법은 각 보안등급의 사용자가 정확한 참조 관계의 유지를 위해 더 많은 책임을 져야한다는 단점은 있지만, 참조 모호성 문제와 다단계 관계형 데이타베이스의 모델링 능력의 제한을 동시에 극복하는 장점이 있다.

현재 대부분의 관계형 데이타베이스 시스템은, 서론에서 지적한 바와 같이, 대부분 임의적 접근제어 모델에 기반하고 있으나, Oracle, Sybase 등의 제품에서는 단일 릴레이션에 대한 다단계보안 모델도 추가적으로 지원하고 있다. 이는 응용 영역에 따라 임의적 접근제어 모델에 비해 다단계보안 모델이 보안 정책을 유지, 관리하는데 유리한 경우가 있기 때문이다. 이와 관련하여 SQL3등의 표준에도 언젠가는 다단계보안 모델의 지원 여부에 대한 논의가 이루어지리라 본다. 이 경우에 관계형 데이타모델의 핵심 무결성 사항인 참조 무결성에 관한 고려가 있어야 할 것이고, MLS-RIS는 하나의 대안이 될 수 있으리라 본다. 그리고, [2] 에 나와 있듯이, MLS-RIS를 다단계보안 관계형 데이타모델상에서 조인의 의미를 정의하는데 적용할 수 있고, 다단계 릴레이션간의 효율적인 조인 알고리즘을 개발에 응용할 수도 있다.

5. 결 론

본 저자들은, 다단계 보안 관계형 데이타 모델에서의 참조 무결성에 관한 연구는 SQL 표준의 동적 의미론 규칙의 확장을 반드시 고려해야 한다고 본다. 또한 참조 모호성의 문제에 대해, [21,24] 에서처럼 참조 모호성의 문제를 회피(avoidance)하거나 데이타베이스 스키마의 모델링 능력을 제한하는 방법은 정상적인 해결책이 아니라고 생각한다. 이에, 우리는 본 논문에서 다단계 관계형 데이타 모델을 위한 확장된 참조 무결성 의미론 **MLS-RIS**를 제안했다. 우선, SQL 표준의 참조 무결성과 참조 무결성 유지를 위한 동적 의미론을 다단계 보안 모델에서 발생하는 다중인스턴스화된 개체나 다중인스턴스화된 속성에 의한 참조 모호성의 해결을 위한 규칙을 제시했다. 그리고, 이 해결 규칙에 기반하여 R_C, R_P에 투플의 삽입, 삭제, 변경 연산과 세가지의 외래키 명세 사양, 즉 **CASCADE**, **RESTRICT**, **SET**

NULL의 각 조합에서 참조 무결성을 유지하는 의미론을 정의하였다.

본 연구내용에 기반하여 우리는 향후 다음의 두가지 방향의 연구를 진행할 예정이다. 첫째, 현재의 MLS-RIS보다 유연한(flexible)한 참조 관계를 지원하기 위해 표준 SQL의 외래키 명세 구문의 확장 방안을 모색할 것이다. 현재의 MLS-RIS는 해결 규칙의 도입을 통해 참조 모호성을 해결한 첫번째 시도이지만, 사용자 입장에서는 다단계 릴레이션들사이의 다양한 참조 관계의 표현을 필요로 한다. 따라서, 다단계 릴레이션들의 정의시에 외래키 선언 명세사양의 확장을 통해 사용자가 원하는 의미론을 지원하고자 한다 이는 보안정책(security policy)의 다양성을 지원한다는 측면에서[15]의 연구와 맥락을 같이 한다. 두번째 연구로는, 본 MLS-RIS에서 제시한 참조 무결성의 동적 의미론과 관련하여, 데이타베이스내에 여러개의 참조관계가 존재할 때 야기될 수 있는 참조 관계의 전역적인 참조 모호성(global referential ambiguity) 문제의 해결을 위한 연구를 할 예정이다. 현재의 SQL 표준이나 MLS-RIS 모두, 하나의 참조 관계의 동적 의미론은 상대적으로 직관적이고 이해하기 쉽다. 하지만, [5,19,22] 등의 연구에서 지적한 바와 같이, 한 트랜잭션이 여러개의 연관된 참조관계들에 영향을 미칠 때, 이들 참조 관계성의 동적 의미론에 의한 연산들이 서로 다른 순서로 실행될 때, 서로 다른 최종 결과를 초래할 수 있다. 따라서, 현재의 MLS-RIS를 기반으로 전역적인 참조 모호성의 해결을 위한 프레임워크를 개발하고자 한다.

참 고 문 헌

[1] 이 상원, 김 형주. "객체지향 데이타모델에서 다중사례화를 위한 버전 개념 확장". 정보과학회 논문지, 21(2), 1994.

[2] 김 용한. "다단계보안 관계형 데이타모델의 참조무결성과 조인 시맨틱스".서울대 공학석사학위 논문, 1997.

[3] J. Banerjee et al. "Data Model Issues for Object-Oriented Applications". ACM Transaction on Office Information Systems, 5(1), Jan., 1987.

[4] D.E. Bell, L.J. LaPadula. "Secure Computer Systems: Unified Exposition and Multics Interpretation". Technical Report MTIS AD-A023588, 1975.

[5] R. Cochrane, H. Pirahesh, N. Mattos. "Integrating Triggers and Declarative Constraints in SQL Database Systems" Proceedings of International Conferences on Very Large Data Bases, 1996.

[6] E. F. Codd. "A Relational Model of Data for Large Shared Data Banks". Communications of ACM, 13(6), 1970.

[7] C. J. Date. "Referential Integrity". Proceedings of International Conferences on Very Large Data Bases, 1981.

[8] R. David, S. Son, R. Mukkamala. "Supporting Security Requirements in Multilevel Real-Time Databases". Proceedings of IEEE Symposium on Research in Security and Privacy, 1995.

[9] Dorothy E. Denning, T. F. Lunt et al. "The SeaView Security Model". Proceedings of IEEE Symposium on Research in Security and Privacy, 1988.

[10] Ronald Fagin "On an Authorization Mechanism". ACM Transactions on Database Systems, 3(3), Sep., 1978.

[11] G. E. Gajnak. "Some Results from the Entity-Relationship Multilevel Secure DBMS Project". Aerospace Computer Security Applications Conference, 1989.

[12] Binto George, Jayant Haritsa. "Secure Transaction Processing in Firm Real-Time Database Systems". Proceedings of the ACM SIGMOD, 1997.

[13] ISO-ANSI Working Draft. "Database Language SQL(SQL/Foundation)".http://ftp.digital.com/pub/standards/sql/sql-foundation-aug94.txt, 1994.

[14] J. Melton, A. R. Simon "Understandng The New SQL: A Complete Guide". Morgan Kaufmann, 1993.

[15] Sushil Jajodia, Pierangela Samarati, V. S. Subrahmanian, Elisa Bertino, "A Unified Framework for Enforcing Multiple Access Control Policies", Proceedings of the ACM SIGMOD, 1997.

[16] Sushil Jajodia, Ravi Sandhu. "Polyinstantiation Integrity in Multilevel Relations". Proceedings of IEEE Symposium on Research in Security and Privacy, 1990.

[17] Sushil Jajodia, Ravi Sandhu. "Update Semantics for Multilevel Relations". IEEE, 1990.

[18] Sushil Jajodia, Ravi Sandhu. "A Novel Decomposition of Multilevel Relations Into Single-Level Relations". Proceedings of IEEE Symposium on Research in Security and Privacy, 1991.

[19] Bertram Lud, Wolfgang May, Georg Lausen. "Referential Actions as Logical Rules". Proceedings of ACM International Conferences on PODS, 1997.

[20] Teresa F. Lunt. "Polyinstantiation: an Inevitable Part of a Multilevel World" Proceedings of the Fourth Workshp on the Foundations of Computer Security, 1991.

[21] T. F. Lunt, Dorothy E. Denning et al. "The SeaView Security Model". IEEE Transactions on Software Engineering, 16(60, 1990.

[22] Victor M. Markowitz, "Safe Referential Integrity Structures in Relational Databases". Proceedings of International Conferences on Very Large Data Bases, 1991.

[23] Fausto Rabitti et al. "A Model of Authorization for Next-Generation Database Systems". ACM Transactions on Database Systems, 16(1), Mar., 1991.
[24] Ravi Sandhu, Sushil Jajodia. "Referential Integrity in Multilevel Secure Databases". Proc. of 16th NIST-NCSC National Computer Security Conference, Baltimore, 1993.
[25] S. Son, B. Thuraisingham. "Towards a Multilevel Secure Database Management System for Real-Time Applications". Proc. of IEEE Workshop on Real-Time Applications, 1993.
[26] Paul D. Stachour, Bahvani Thuraisingham. "Design of LDV: A Multilevel Secure Relational Database Management System". IEEE Transactions on Knowledge and Data Engineering, 2(2), 1990.
[27] M. B. Thuraisingham. "Mandatory Security in Object-Oriented Database Systems". Proceedings of OOPSLA, 1989.

이 상 원
1991년 서울대학교 컴퓨터공학과 학사 졸업. 1994년 서울대학교 컴퓨터공학과 석사 졸업. 1994년 ~ 현재 서울대학교 컴퓨터공학과 박사 과정 재학. 관심분야는 데이타베이스, 데이타웨어하우스, 컴퓨터 보안.

김 용 한
1995년 아주대학교 컴퓨터공학과 학사 졸업. 1997년 서울대학교 컴퓨터공학과 석사 졸업. 1997년 ~ 현재 한국 오라클 근무. 관심분야는 데이타웨어하우스, 컴퓨터 보안.

김 형 주
제 25 권 제 2 호(B) 참조