비공간 정보와 보안 등급을 갖는 공간 객체를 위한 다중인스턴스 기법

(A Polyinstantiation Method for Spatial Objects with Several Aspatial Information and Different Security Levels)

오 영 환 † 전 영 섭 †† 조 숙 경 ††† 배 해 영 ††††
(Young-Hwan Oh) (Young-Sub Jun) (Sook-Kyoung Cho) (Hae-Young Bae)

요 약 공간 데이타베이스 시스템에서는 동일한 레이어 상에서 보안등급이 다른 두개 이상의 비공간 정보로 이루어진 공간 객체를 관리할 필요성이 있다. 이러한 공간 객체 관리를 위해 관계 데이타베이스 시스템의 다중인스턴스화(polyinstantiation) 기법을 적용하면 공간 객체의 표현상 문제와 상이한 보안등급을 가지는 주체의 접근으로 인한 서비스 거부(service denial)와 정보 노출(information flow)이라는 문제가 발생한다.

본 논문에서는 이와 같은 문제점을 해결하기 위해 상이한 접근등급을 갖는 공간 객체를 위한 다중인스턴스화 기법을 제안한다. 제안된 기법은 공간 객체에 대해 보안등급 변환검사 단계와 다중인스턴스 생성 단계를 통하여 사용자의 등급에 따라 새로운 공간 객체를 생성하고, 이를 보안 정책에 활용한다. 또한 상이한 등급의 사용자가 공간 객체에 대하여 다양한 보안 연산을 요구할 경우 발생하는 서비스 거부와 정보 노출의 문제점을 각 등급에 따른 공간 객체 다중인스턴스를 생성하여 해결한다.

키워드 : 공간 데이타베이스, 데이타베이스 보안, 정보 노출, 다중인스턴스화

Abstract In the spatial database systems, it is necessary to manage spatial objects that have two or more aspatial information with different security levels on the same layer. If we adapt the polyinstantiation concept of relational database system for these spatial objects, it is difficult to process the representation problem of spatial objects and to solve the security problem that is service denial and information flow by access of subject that has a different security level.

To address these problems, we propose a polyinstantiation method for security management of spatial objects in this paper. The proposed method manages secure spatial database system efficiently by creating spatial objects according to user's security level through security-level-conversion-step and polyinstantiation-generation-step with multi-level security policy. Also, in case of user who has a different security level requires secure operations, we create polyinstance for spatial object to solve problems of service denial and information flow.

Key words : Spatial Database, Database Security, Information Flow, Polyinstantiation

1. 서 론

데이타베이스 보안(database security)이란 데이타베이스에 저장된 데이타에 대해서 권한이 없는 액세스, 고의적인 파괴 혹은 변경 그리고 비일관성을 발생시키는 우발적인 사고로부터 데이타 또는 데이타베이스를 보호하는 것이다[1,2]. 이러한 데이타베이스 보안은 최근 들어 시설물 관리, 항공 관제, 군사 시설물 관리 등의 분야에서 공간 데이타베이스 시스템과 혼합되어 사용되어 그 영역을 점차 넓혀가고 있다. 현재까지 데이타베이스 보안 분야에 대한 많은 연구들이 수행되어 왔지만 공간 데이타베이스를 위한 보안에 대한 연구는 미흡하며[3,4], 일반적으로 기존의 데이타베이스 보안 분야의 접근 제어 정책중의 하나인 다중인스턴스화(polyinstantiation) 기법을 적용하여 사용한다[5,6].

† 비 회 원 : 나사렛대학교 교수
yhoh@kornu.ac.kr
†† 비 회 원 : (주)케이지아이 연구원
inhaop@hitel.net
††† 비 회 원 : 인천대 초빙 교수
skyoe@dreamwiz.com
†††† 종신회원 : 인하대학교 컴퓨터공학부 교수
hybae@inha.ac.kr
논문접수 : 2002년 9월 16일
심사완료 : 2003년 9월 26일

공간 데이타베이스 시스템에서 공간 객체는 일반적으로 레이어(layer) 단위로 관리되고, 하나의 공간 객체는 하나의 레코드로 저장되며 공간(spatial), 비공간(aspatial) 정보가 일대일 형식으로 연결된 형태로 관리된다. 하지만 실세계에는 동일한 레이어 상의 공간 객체 중에서 보안등급(security level)이 다른 두 개 이상의 비공간 정보로 이루어진 공간 객체(spatial object)가 존재한다. 예를 들어, 실세계에는 3층으로 지어진 건물(공간 데이타, SO)이 있고, 이 건물 내에 각층별로 TS(Top-Secret)등급의 안보기관(A1), S(Secret)등급의 은행(A2), U(Unclassified)등급의 일반 상가(A3)의 서로 다른 보안등급을 가지는 속성데이타로 표현되는 건물이 존재한다. 이 3층 건물은 레이어에서 하나의 공간 데이타(S0)로 관리되며, 이들 3개의 기관들은 모두 동일한 위치 정보로 표현된다. 서로 다른 보안등급을 가지는 사용자에 의한 공간 객체에 대한 접근은 결과적으로 모두 동일한 연산으로 처리된다. 이 때, 본 논문에서는 공간 데이타(S0)의 변경 연산은 고려하지 않는다. 공간 데이타는 공간 객체의 표현만을 위해 존재하도록 한다.

높은 보안등급의 사용자가 낮은 등급의 공간 객체를 접근할 시 비밀 채널을 통해 공간 정보의 노출이 발생할 수 있으며, 반대의 경우로 낮은 보안등급을 가진 사용자에 대한 접근 거부가 발생할 수 있다. 이는 Bell-Lapaula 모델의 제약 조건인 단순 속성(simple property)과 제한된 *-속성(limited *-property)에 따른다. 단순속성은 주체(사용자)의 보안등급이 객체(데이타)의 보안등급과 동일하거나 높은 경우에만 판독연산을 허용하는 것이며, 제한된 *-속성은 주체의 보안등급이 객체의 보안등급과 동일한 경우에만 갱신연산을 허용한다. Bell-Lapadula 모델의 두 가지 속성은 허가되지 않은 사용자에게 직접적으로 기밀 데이타를 유출하는 것을 막을 수 있으나, 간접적인 비밀 누출을 통한 불법적인 정보의 흐름인 비밀 누출(covert channel)을 방지할 수 없다[7]. 이를 해결하기 위한 방법으로 다중인스턴스화 기법을 제안하나 기존의 관계 데이타베이스 시스템의 다중인스턴스화 기법을 보안 공간 객체(secure spatial object) 유지에 그대로 사용하게 되면 서비스 거부, 정보 노출과 같은 문제점이 발생한다.

본 논문에서는 이러한 문제점을 해결하기 위해, 공간 객체에 대한 다중인스턴스화 기법을 제안한다. 제안하는 기법은 기존 관계 데이타베이스 시스템의 다중인스턴스화 기법을 확장하여 다단계 보안 공간 객체를 효율적으로 표현하며, 이 객체에 대한 서비스 거부와 정보 노출을 방지한다. 이 기법은 보안등급 변환검사 단계와 다중인스턴스 생성 단계로 구성된다. 보안등급 변환검사 단계에서는 공간 객체에 대한 보안등급과 이 객체에 대한 접근을 요구한 사용자의 보안등급을 서로 비교하여, 상향 변경(forward modification) 또는 하향 변경(downward modification)을 판별하는 단계이다. 상향 변경이라는 것은 새로 생성될 비공간 데이타의 보안등급이 사용자가 요구한 보안등급 보다 높은 경우 수행하는 연산을 말하며, 하향 변경은 이 반대의 경우를 말한다. 다중인스턴스 생성 단계는 보안등급 복사, 비공간 데이타 복사 및 공간 객체 식별자 복사의 순서로 진행된다. 보안등급 복사는 사용자의 보안등급을 복사하는 과정이며, 비공간 데이타 복사는 상향 변경인 경우는 보안등급을 제외한 나머지 비공간 필드를 복사하고 하향 변경인 경우는 나머지 비공간 필드들을 모두 널(NULL)로 채우는 과정이다. 공간 객체 식별자 복사과정을 통해 객체 식별자를 생성하며 객체 식별자와 보안등급을 복합키(composite key)로 묶어서 사용한다. 제안된 기법은 기존의 관계 데이타베이스 시스템의 다중인스턴스화 기법을 공간 데이타베이스 시스템에서 효과적으로 사용할 수 있도록 확장한 새로운 기법이다.

본 논문의 구성은 제2장에서 관련연구로 접근 제어 정책과 다중인스턴스화 기법에 대해 알아보고 제3장에서 공간 객체의 다중인스턴스화 기법을 제안한다. 제4장에서 공간 객체의 다중인스턴스에 대한 관리정책을 설명한다. 마지막으로 제5장에서 결론을 맺는다.

2. 관련 연구

본 장에서는 접근 제어를 위한 임의적 접근 제어(discretionary access control)와 강제적 접근 제어(mandatory access control)에 대해 설명하고, 다단계 보안을 위한 관계형 데이타베이스 시스템에서의 다중인스턴스화 기법에 대해 설명한다.

2.1 접근 제어

사용자 접근 제어를 위한 보안 방식은 임의적 접근 제어와 강제적 접근 제어로 크게 구분할 수 있다. 임의적 접근 제어는 주체나 주체가 속해있는 그룹들의 식별자를 근거로 객체에 대한 접근을 제한하는 방법이며, 강제적 접근 제어는 객체에 포함된 등급별 비밀 취급 인가를 기반으로 하여 객체에 대한 접근을 제어하는 방법이다. 강제적 접근 제어는 다단계 보안 기법 구현을 위한 방법론의 핵심이 된다.

강제적 접근 제어는 주체(subject)와 객체(object)라는 용어에 의해 기술된 Bell-Lapadula 모델에 기초한다[8,9]. 객체는 데이타화일, 레코드 또는 레코드 내의 필드로 이해될 수 있으며, 주체는 객체들에 대한 액세스를 요청할 수 있는 활성화된 프로세스이다. 모든 객체는 비밀 등급이 할당되며, 각각의 주체도 등급별 비밀취급 인가가 되어야 한다. 안전한 시스템은 데이타에 대한 직접

적인 비밀 누출 뿐만 아니라, 간접적인 비밀 누출을 통한 불법적인 정보의 흐름을 차단할 수 있어야 한다. 비밀 채널(covert channel)이 후자에 속하는 간접적인 비밀 누출의 형태이다. 비밀 채널은 상위 비밀 취급 인가자가 하위 비밀 취급 인가자에게 간접적인 정보 누출 수단을 제공할 수 있다.

강제적 접근 제어는 다단계 데이타베이스 보안 시스템의 주된 제어 방식으로 각 시스템의 주체와 객체에게 보안등급을 부여하고, 등급별로 분리된 정보가 하위로 흘러 내려가는 것을 방지하는 접근제어 기법이다[10].

2.2 다중인스턴스화

다중인스턴스는 동일한 이름을 갖는 데이타 객체가 동시에 여러 개 존재하는 것으로, 높은 접근 등급의 사용자의 행위가 낮은 접근 등급의 사용자에게 알려지지 않도록 함으로써 비밀채널을 방지 시킨다[11-13]. 다중인스턴스는 다단계 보안 시스템의 본질적인 현상으로 관계형 데이타베이스의 릴레이션, 튜플 및 필드에 영향을 미치며, 튜플 수준과 필드 수준에서 정의할 수 있다[14]. 다중인스턴스화는 다단계 릴레이션, 강제적 보안, 여과의 자연스러운 결과이다. 다중인스턴스화 데이타를 주체가 완전히 알아채지 못하는 방법으로 다중인스턴스화를 유지해야 한다.

다음 표 1은 다중인스턴스화의 예를 보여준다[15]. 표 1은 다중인스턴스화 종류 중에서 가장 세밀한 접근 방법으로 다중인스턴스화 속성값(polyinstantiation entity)이다. 이는 주키, 키 보안등급, 그리고 속성값 보안등급에 의해 구별되는 속성값들로 보안등급은 다르지만 같은 [주키, 키 보안등급]의 쌍과 연관되는 속성에 대하여 많은 값들이 존재할 수 있다. 예를 들어, '아리안' 우주선은

표 1 다중인스턴스화 속성값의 예

STARSHIP	PURPOSE	DESTINATION	TC
아리안 *u*	탐험 *u*	화성 *u*	*u*
아리안 *u*	채광 *c*	금성 *u*	*c*
아리안 *u*	정찰 *s*	목성 *u*	*s*
아리안 *u*	공격 *ts*	토성 *u*	*ts*

그 목적에 따라 속성값 보안 등급이 다를 수 있다. 또한 속성값 보안등급에 따라 튜플 보안등급이 달라진다.

3. 공간 객체를 위한 다중인스턴스화 기법

본 장에서는 다단계 보안 공간 객체에 대한 정의를 하고 공간 객체의 무결성 유지와 보안 관리를 위한 공간 객체의 다중인스턴스 구조를 정의한다.

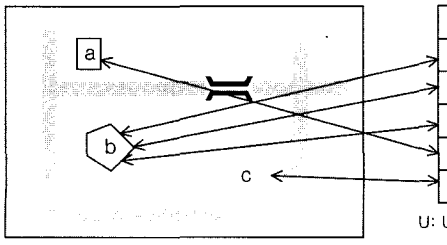
3.1 다단계 보안 공간 객체

공간 객체는 일반적으로 레이어 단위로 관리되며, 이러한 레이어에서 하나의 공간 객체는 하나의 레코드로 저장되며 공간 정보와 비공간 정보가 일대일 형식으로 연결된 형태로 관리된다. 하지만 실세계에는 동일한 레이어 상의 공간 객체 중에서 보안등급이 다른 두개 이상의 비공간 정보로 이루어진 공간 객체가 존재한다. 예를 들어, 도면상에 표현되는 공간 객체는 이차원 평면 위에 다각형 형태로 표현이 되기 때문에 공간 객체에 대한 속성 정보는 비공간 정보를 통해서 확인 가능하다. 즉, 1층 건물이든 다층 건물이든 하나의 다각형으로 표현되기 때문에 고층 건물이 보안등급을 달리하는 정보를 가진 사무실로 구성되어 있을 경우에는 보안등급이 다른 사용자별로 자신이 접근 가능한 정보를 보여줄 필요가 있다.

그림 1은 상이한 보안 등급을 갖는 공간 객체의 예로서 이차원 형태로 표현되는 도면이라고 가정하자. 공간 객체(a)는 U 등급의 경찰서(A1)를, 공간 객체(b)는 U 등급의 일반 상가(B1), S 등급의 벤처 타운(B2), TS 등급의 정보 기관(B3) 그리고 공간 객체(c)는 TS 등급의 정보 기관(C1)을 가리킨다. 공간 객체 (b)와 같은 경우에는 보안등급이 다른 3개의 비공간 정보를 가지고 있다. 위와 같은 경우는 실제로는 여러 층으로 이루어진 빌딩이지만, 이차원 평면상에 표현할 경우에는 하나의 공간 데이타로 표현할 수 밖에 없다.

3.2 공간 객체의 다중인스턴스화

공간 객체 다중인스턴스화 기법은 관계 데이타베이스 시스템의 다중인스턴스화 기법을 확장하여 공간 객체에



(a) 객체 표현

ID	명칭	보안등급
B1	일반상가	U
B2	벤처타운	S
B3	정보기관	TS
A1	경찰서	U
C1	정보기관	TS

U: Unclassified, C:Confidential, S:Secret: TS:Top Secret

(b) 테이블 구조 표현

그림 1 다단계 보안 등급을 갖는 공간 객체의 예

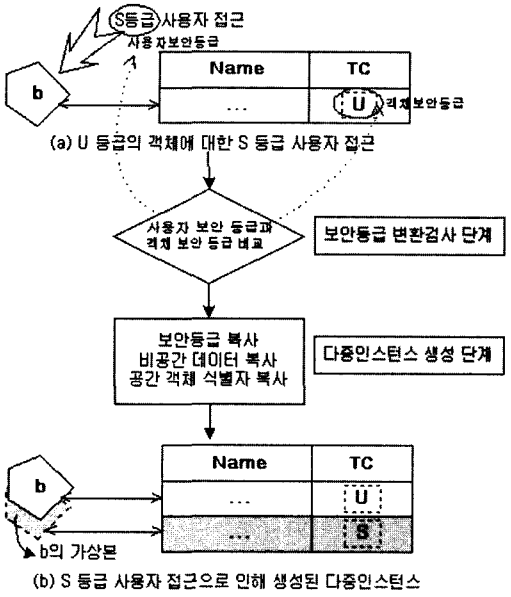


그림 2 공간 객체 다중인스턴스화

대한 간접적인 비공간 정보의 노출을 방지할 수 있다. 그림 2는 공간 객체 다중인스턴스화 기법에 대한 그림이다.

공간 객체 다중인스턴스화 기법의 처리과정은 보안등급 변환검사 단계와 다중인스턴스 생성 단계로 구성된다. 보안등급 변환검사는 공간 객체에 대한 보안등급과 이 객체에 대한 접근을 요구한 사용자의 보안등급을 서로 비교하여, 객체의 보안등급에 대해 상향 변경 또는 하향 변경을 판별하는 단계이다. 상향 변경이라는 것은 새로 생성될 공간 데이타의 보안등급이 사용자가 요구한 보안등급 보다 높은 경우 수행하는 연산을 말하며, 하향 변경은 이 반대의 경우를 말한다. 상향 변경 단계는 낮은 보안등급을 가진 객체에 대하여 높은 보안등급을 가진 사용자가 접근시 데이타의 무단 변경으로 인한 정보 노출을 막기 위한 단계이다. 하향 변경 단계는 반대의 경우로 낮은 보안등급을 가진 사용자에 대한 접근 거부로 발생하는 서비스 거부를 해결하기 위한 단계이다.

그림 3(a)에서 S등급의 사용자가 U등급을 가진 객체에 대하여 검색 연산을 요구할 경우, 판독이 가능하다. 그러나, 속성 데이타에 대한 변경 연산을 요구할 경우, S등급의 사용자가 강제적으로 U등급의 비공간 데이타를 변경하므로 정보 노출이 발생한다. 이는 Bell- Lapadula의 제한된 *-속성제약 조건에 근거한다. 이를 위해 S등급을 갖는 공간객체 다중인스턴스를 생성하여 정보 노출을 방지시킨다. 즉, 보안등급 변환검사 단계에서 사용자의 보안등급과 객체의 보안등급이 다르다는 결과가 나온 후 다음 단계인 다중인스턴스 생성 단계로 넘어가게 된다. 다중인스턴스 생성 단계는 보안등급 복사, 비공간 데이타 복사, 공간 객체 식별자 복사의 순서로 진행된다. 보안등급 복사는 변경된 보안등급, 즉 접근한 사용자의 보안등급으로 채우는 과정이다. 비공간 데이타 복사는 보안등급을 제외한 나머지 비공간 필드를 복사한 후 '일반 상가'(U)를 '정보기관'(S)으로 데이타 값을 변경한다. 그리고 공간 객체 식별자를 복사한다.

이 경우, 공간 데이타 값을 복사하지 않고 객체 식별자를 복사하는 이유는 다음과 같다. 일반적으로 공간 데이타는 비공간 데이타와 달리 벡터 기반의 대용량 저장구조를 가지며, 실제적으로 비공간 데이타에 비해 수 백에서 수 십만 배의 기억용량을 소비한다. 그리고, 본 논문에서는 공간 데이타의 변경을 고려하지 않기 때문에 이를 중복해서 저장할 필요가 없으며 보안 등급이 다른 여러 주체가 다수의 비공간 정보를 접근하더라도 이에 대한 공간 정보는 동일하므로 중복할 필요가 없다. 따라서, 공간 객체에 대한 식별자만을 복사함으로써 데이타의 일관성을 유지하도록 한다.

그림 3(b)와 같이 U등급을 가진 사용자가 S등급의 공간 객체를 검색하였을 경우, 공간 데이타와 속성 데이타 전부 판독이 불가능하다. 그러나, 공간 데이타가 사용자 화면에 출력되지 않는다면, 낮은 등급의 사용자는 높은 등급의 공간 데이타가 그 지역에 위치하고 있음을

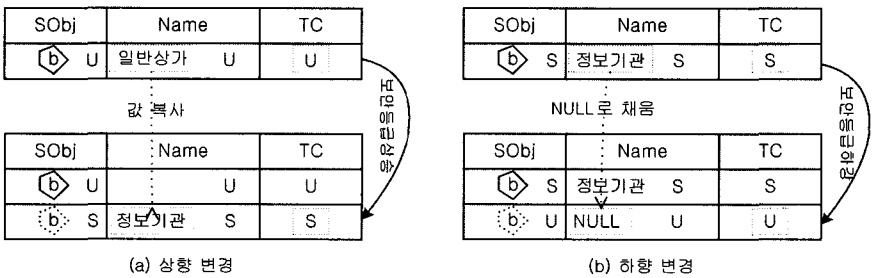


그림 3 공간 다중인스턴스 생성을 위한 등급 변환과정

유추할 수 있다. 이를 통해 간접적인 정보 노출이 발생한다. 또한 공간 데이타에 대한 서비스 거부 문제가 발생한다.

이와 같은 하향 변경인 경우, U등급을 위한 다중인스턴스 생성 단계는 보안등급 복사, 비공간 데이타 복사, 공간 객체 식별자 복사의 순서와 같이 상향 변경과 동일하게 진행된다. 그러나 비공간 데이타 복사는 보안등급을 제외한 나머지 비공간 필드를 NULL로 변경하여 정보 노출을 방지한다.

4. 공간 객체의 연산을 위한 다중인스턴스 관리 정책

본 장에서는 공간 객체에 대한 검색, 삽입, 갱신 및 삭제 연산을 위한 다중인스턴스 관리 정책을 설명하고, 다단계 보안 관리에 대해서도 공간 객체 다중인스턴스를 이용해서 설명한다.

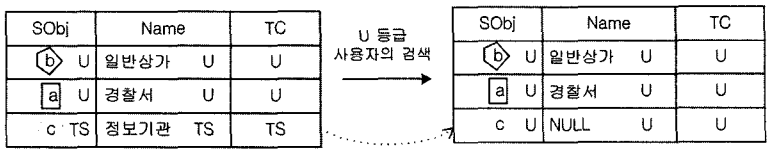
공간 객체 다중인스턴스는 다단계 보안을 적용하는 공간 데이타베이스 시스템에서 상이한 등급의 사용자들에게 보안등급이 다른 객체에 대한 접근 제어를 목적으로 생성하는 것이다. 공간 객체 다중인스턴스화 기법을 이용해서 생성된 객체에 대한 연산을 위해서는 다중인스턴스 관리 정책이 수반되어야 한다.

4.1 검색 연산

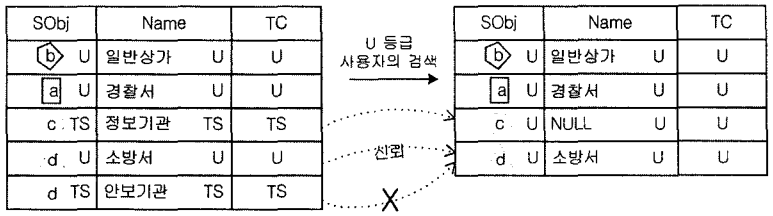
다음 그림 4에서 공간 객체 다중인스턴스가 존재하지 않는 경우(a)와 존재하는 경우(b)에 대한 검색 연산시 관리정책을 설명한다. (a)의 경우에는 사용자의 보안등급보다 높은 보안등급을 가지는 객체의 비공간 필드에 대해서는 NULL값으로 보여주고, 공간 정보는 숨기는 것 자체가 정보 노출을 가능하게 하기 때문에 공간 정보는 동일하게 보여주도록 한다. 그리고 (b)처럼 공간 복합객체 다중인스턴스가 존재할 경우에는 접근이 허용된 모든 객체 정보를 보여주는 것이 아니라 보안등급 변환검사 단계에서 접근한 사용자의 보안등급과 비교하여 동일한 보안등급의 객체 정보만을 보여주도록 한다.

4.2 삽입 연산

삽입 연산 과정은 테이블에 접근한 보안등급을 가진 사용자의 보안등급만을 고려한다. 즉, 보안등급 변환검사 단계에서 객체의 보안등급과 비교할 필요가 없다. 삽입 연산은 다중인스턴스 생성단계를 거치지 않고, 공간 객체를 생성한다. 즉 튜플 보안등급 삽입, 비공간 데이타 삽입, 공간데이타 삽입 순의 연산을 거쳐 하나의 공간 객체를 새로 생성하게 된다. 그림 5의 초기 테이블(a)에서 TS등급의 사용자가 공간 객체 d를 삽입하고 비공간 정보를 입력한 후, 결과테이블(b)에 새로운 객체

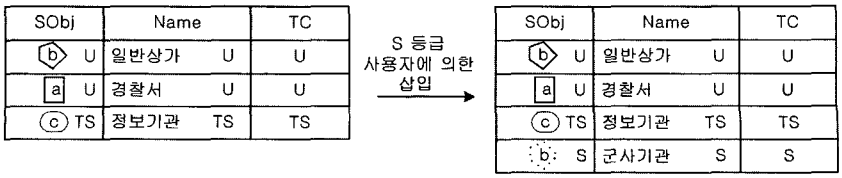


(a) 공간 복합객체 다중인스턴스 데이터가 존재하지 않을 경우



(b) 공간 복합객체 다중인스턴스 데이터가 존재할 경우

그림 4 검색 연산을 위한 다중인스턴스 관리 정책



(a) 초기 테이블 (b) 결과 테이블

그림 5 삽입 연산을 위한 관리 정책

d가 생성된다.

4.3 갱신 연산

그림 6과 같이 갱신 연산의 경우는 크게 세 가지 경우로 살펴볼 수 있다. 사용자의 보안등급과 객체의 보안등급이 동일한 경우(a), 보안등급이 높은 사용자가 보안등급이 낮은 객체를 갱신하는 경우(b), 그리고 보안등급이 낮은 사용자가 보안등급이 높은 객체를 갱신하는 경우(c)로 나눌 수 있다. 이 세 가지 경우에 대한 다중인스턴스 관리정책은 다음과 같다.

(1) 사용자 보안등급 = 객체 보안등급

그림 6(a)의 TS 등급을 가진 c 객체에 대하여 TS 등급의 사용자가 갱신 연산을 요구할 경우, 다중인스턴스를 생성하는 것이 아니라 현재 레코드에 대한 갱신을 수행한다.

(2) 사용자 보안등급 > 객체 보안등급

그림 6(b)의 S등급을 가진 d객체에 대해 TS등급의 사용자가 갱신 연산을 요구할 경우, 사용자는 객체에 대해 접근은 가능하지만 그 객체에 대한 레코드를 갱신하지 않는다. 이와 같은 경우에는 접근된 공간 객체에 대한 다중인스턴스를 생성한다. 즉, 접근하는 주체의 보안등급이 객체의 보안등급보다 높은 경우, 공간 객체에 접근할 수 있다. 그러나 만일 보안등급이 높은 주체가 낮은 보안등급의 객체에 대한 정보를 강제적으로 갱신한다면, 보안등급이 낮은 사용자가 이 객체에 대해 접근을 하려고 할 때 간접 정보 노출의 문제가 발생하게 된다. 상향 변경의 공간객체 다중인스턴스 기법에 따라 d객체에 대한 공간 객체식별자가 복사된 후, TS등급을 변경되고, 사용자가 원하는 비공간 데이타 값 '정보기관'을 입력한다. 그리고 튜플 보안등급을 TS등급으로 설정한다.

(3) 사용자 보안등급 < 객체 보안등급

그림 6(c)의 S등급을 가진 d객체에 대해 U등급의 사용자가 갱신 연산을 요구할 경우, 공간 객체의 보안등급이 높다고 해서 서비스를 거부하는 것이 아니라 다중인스턴스를 생성함으로써 갱신 연산을 정상적으로 수행하

그림 6 갱신 연산을 위한 다중인스턴스 관리 정책

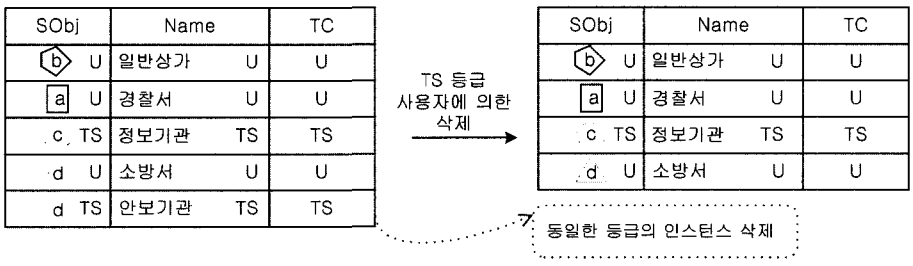


그림 7 삭제 연산을 위한 다중인스턴스 관리 정책

도록 한다. 이처럼 사용자의 보안등급이 객체의 보안등급보다 낮은 경우, 보안등급이 낮은 사용자가 갱신을 위하여 공간 객체에 접근할 경우 상위 보안등급의 객체 존재로 인한 갱신 거부, 즉 서비스 거부의 문제가 발생한다. 따라서 이와 같은 경우에는 서비스 거부를 막기 위해 보안등급 변환검사 단계의 하향변경과 다중인스턴스 생성 단계를 거쳐 공간 객체 다중인스턴스를 생성한다. d객체에 대하여 보안 등급을 사용자 보안등급(U)으로 설정하고 사용자가 입력하기 원하는 값 '소방서'를 입력한다. 그 후 튜플 보안등급을 U로 설정한다.

4.4 삭제 연산

삭제 연산에서는 공간 복합객체의 보안등급과 객체의 보안등급이 동일할 경우에만 삭제가 가능하도록 한다. 이는 Bell-Lapadula 모델의 *-속성을 따르는 것으로 불법적인 사용자의 접근으로부터 보안을 유지하기 위해서이다.

5. 결 론

본 논문에서는 공간 객체의 표현과 서비스 거부, 정보 노출이라는 보안 문제를 해결하기 위해 공간 객체에 대한 다중인스턴스화 기법을 제안하였다.

공간 다중인스턴스화 기법은 보안등급 변환검사와 다중인스턴스 생성단계로 구성되며, 보안등급 변환검사 단계에서는 갱신 연산을 위해 공간 객체에 접근시 사용자와 객체의 보안등급을 비교하였다. 그리고 보안등급이 서로 다를 경우 다중인스턴스 생성 단계에서 공간 및 비공간 데이타를 상향변경 및 하향변경에 따라 객체를 생성하도록 하였다. 즉, 공간 객체 다중인스턴스를 생성함으로써 공간 객체에 대한 상이한 보안 주체에 대한 표현을 가능하게 하였다. 그리고 공간 다중인스턴스 관리 정책을 이용하여 데이타 갱신 시 발생하는 서비스 거부와 정보 노출의 문제점을 사용자의 등급에 따른 공간 객체 다중인스턴스를 생성함으로써 해결하였다.

참 고 문 헌

[1] Guerrini, G., Bertino, E., Catania, B., and Garcia-Molina, G., "A Formal Model of Views for Object-Oriented Database Systems," *Technical Report*, DISI-96-2, 1996.

[2] Jajodia, S., "Database Security : Current Status and Key Issues," *SIGMOD Record*, Vol.19, No.4, pp.123-126, 1990.

[3] 전영섭, 오영환, 이순조, 임기욱, 배해영, "다단계 보안을 갖는 공간 뷰를 이용한 정보 흐름 제어", 정보처리학회 춘계 학술발표논문집 제8권, 제1호, pp.93-96, 2001.

[4] 조완수, "다단계보안을 위한 확장 관계 데이타베이스 시스템 설계", 박사학위 논문, 인하대학교, 1996.

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

[6] Jajodia, S. and Kogan, B., "Integrating an Object-Oriented Data Model with Multilevel Security," *Proc. of IEEE Symposium on Research in Security and Privacy*, 1990.

[7] Sandhu, R., "Lattice-based access control models," *Computer*, 26:9-19, 1993.

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

[9] Lunt, T., "Multilevel Security for Object-Oriented Database Systems," *Database Security III*, pp.199-209, 1990.

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

[11] Jajodia, S., Sandhu, R. and Sibley, E., "Update Semantics for Multilevel Relations," *Proceeding of the Sixth Computer Security Applications Conference*, pp.103-112, 1990.

[12] Lunt, T. and Hsieh, D., "Update Semantics for a Mulitlevel Relational Database System," *Proceeding of the IFIP WG 11.3 Workshop on Database Security*, pp.281-296, 1990.

[13] Sandhu, R. and Jajodia, S., "Eliminating Polyinstantiation Securely," *Computer & Security*, Vol.11, No.6, pp.547-562, 1992.

[14] Miranda, S., "Aspects of Data Security in General-Purpose Database Management Systems," *Proc. of the First Five Symposia 1980-1984*, Vol. I, pp.46-58.

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

오 영 환

1993년 인하대학교 전자계산공학과 학사
1997년 인하대학교 전자계산공학과 석사
2001년 인하대학교 전자계산공학과 박사
2000년~2001년 (주)케이지아이 시스템 개발부 부장. 2002년~현재 나사렛대학교 전임강사. 관심분야는 공간데이타베이스, 데이타베이스 보안, GIS

전 영 섭

2000년 인하대학교 전자계산공학과 학사
2002년 인하대학교 전자계산공학과 석사
2002년~현재 (주)케이지아이 연구원. 관심분야는 공간데이타베이스, 데이타베이스 보안, 지리정보시스템

조 숙 경

1990년 인하대학교 전자계산학과 이학사
1994년 인하대학교 전자계산공학과 석사
2002년 인하대학교 전자계산공학과 박사
2003년~현재 인천대 초빙 교수. 관심분야는 실시간 데이타베이스 시스템, 이동 데이타베이스 시스템, 데이타베이스 보안

배 해 영

정보과학회논문지 : 데이타베이스
제 30 권 제 3 호 참조