通信情報保護學會誌
第6卷 第1號, 1996. 3

객체지향 데이타베이스 체계의 보안성 질의 관리

Secure Queury Management for Object-Oriented Database Systems

최 용 구*, 문 송 천**

요 약

본 논문의 목적은 객체지향 데이타베이스(object-oriented database : OODB)의 보안성 확보를 위하여 OODB에 관련된 보안 모델과, 질의 처리시에 보안성 확보를 위한 참조제약 규칙을 제안하는 것이다. 본 논문의 철학은 데이타베이스 모델의 제약사항을 최소화여 융통성을 최대한으로 확보하고, 이들의 보안성 보장은 질의 처리시에 담당하게 함으로서 풍부한 데이타 객체 모델을 가질 수 있을 뿐만 아니라 낙관적인 보안성 확보를 통하여 융통성 있는 질의처리를 도모하였다. 이를 위하여 현실세계의 모든 개체의 특징과 행위를 구체적으로 표현한 추상화 단위로 정의되는 객체를 기밀성에 따라 비밀등급으로 보안 분류하여 보관된 다단계 보안 객체의 모델을 기반으로 한다. 대부분 기존의 보안성 연구의 대상은 수동적인 데이타(passive data)이라면 객체지향 데이타베이스는 능동적인 객체(active object)가 보안성 연구의 대상이 된다.

1. 서 론

객체지향 데이타베이스는 다양한 응용분야를 지원할 수 있는 풍부한 데이타 객체를 포함하고 있다. 가령 이러한 응용 분야는 복합 객체들의 강력한 모델을 요구하는 다중매체 데이타(multimedia data), 실시간 데이타(real-time data)의 표현과 컴퓨터의 의한 설계 및 제조(computer aided design and manufacturing : CAD/DAM), 그리고 컴퓨터를 통한 소프트웨어 공학(computer aided software engineering : CASE)등이 있다. 이와 같이 OODB가 다양한 응용분야를 지원할 수 있음에도 불구하고 더욱더 이들의 신뢰성 및 안정성의 보장이 강력히 요구되고 있는 실정에 있다. 이를 위해서는 OODB의 보안성 유지에 대한 연구가 불가피하다. 여기서 데이타베이스 보안이란 데이타베이스내에 저장되어 있는 데이타 객체에 대한 권한이 없는 접근, 고의적인 파괴 혹은 변경, 그리고 비일관성을 발생시키는 우발적인 사고로 부터 객체 혹은 데이타베이스를 보호하는 기능으로 정의할 수 있다.

기존의 데이타베이스 보안 단위가 정적인 데이타라고 한다면 OODB는 동적인 특성을 가지고 있는 객체가 보안 연구 단위라는 데에

* 한국과학기술원 정보 및 통신공학과
** 한국과학기술원 정보 및 통신공학과

다른 개념을 가진다. 그리고 OODB는 동적인 스키마 진화특성과 다중판을 자연스럽게 표현할 수 있다는 데에 기존의 데이타베이스와 다른 차원의 보안 연구가 필요하다. 사실 OODB는 객체(object)와 부류(class) 그리고 상속(inheritance)의 개념을 가지고 있다. 객체는 현실세계의 모든 개체(entity)의 특징과 행위를 구체적으로 표현한 추상화 단위이다. 객체는 부류라는 틀로부터 생성된다. 객체를 생성하는 틀[Wagn90]로서 사용되는 부류는 객체의 특징을 표현하기 위한 속성(attribute)의 집합과 그의 행위를 정의하고 있는 방법(method)의 집합으로 구성된다. 그리고 이러한 부류는 다른 속성과 방법들을 추가하여 다른 특성을 가진 부류를 생성할 수 있다. 이러한 개념을 부류의 상속이라고 한다. 부류의 상속은 객체지향 데이타베이스의 스키마진화 뿐만 아니라 속성과 방법의 중복을 제거할 수 있다는 데에 장점을 가지고 있다.

만일 이러한 OODB가 기밀정보를 다루는 기관 혹은 조직에서 고수준의 신뢰성과 안정성 있는 정보체계의 유지를 원한다면 객체의 특징과 행위의 기밀성에 따라서 비밀등급으로 분류하여 저장되고 관리되어야 한다. 이와 같이 비밀등급이 부여된 객체들을 포함하고 있는 OODB를 다단계 보안 OODB시스템(multilevel secure OODB system: MLS/OODBS)[Lunt90, Mill92, Morg92]이라고 한다. 비밀등급으로 분류된 객체는 데이타베이스를 사용하는 주체의 비밀 취급인가 등급에 따라서 접근을 효과적으로 제한할 수 있기 때문에 견고하고 합법적인 보안 관리가 가능하다.

그러나 MLS/OODBS에서 객체들 사이에 상호작용은 직접적인 정보 유출이 가능하다. 왜냐하면 대부분의 객체는 다른 객체들과 관계를 형성하고 있기 때문에 어떤 객체가 참조하고 있는 객체의 정보는 쉽게 노출될 수 있기 때문이다. 이러한 직접적인 정보의 유출은 질의 처리 보안관리기에 의하여 해결되어야 한다.

본 논문에서는 객체모델에서 보안성 보장을 위한 제약사항을 제거한 무제한 상속허용 모델에서 정보의 직접적인 유출을 차단할 수 있는 참조제약 기법을 제시한다. 이러한 참조제약 기법은 질의처리 관리기가 담당하게 된다. 여기서 참조 제약기법은 어떤 부류 계층구조(class hierarchy)에서 객체가 노드를 방문할 때에 방문을 허용(보안상의 문제가 발생하지 않을 경우)할 것인지, 그렇지 않으면 거절(보안상의 문제가 있을 경우)할 것인지를 결정하게 된다. 이러한 접근 방식은 다른 연구[Lunt90, Mill92, Morg92]에서 제시한 것보다 장점을 가지고 있다. 이러한 연구에서는 부류 상속시에 제약을 부여함으로써 데이타베이스에 중복된 의미의 객체가 존재하게 되고, 약한 데이타베이스 모델을 형성하게 된다. 먼저 [Lunt90]와 [Morg92]에서는 보안을 위배하지 못하도록 자신의 객체보다 비밀등급이 낮은 객체의 상속은 이루어지지 못하도록 하였다. 이러한 제약이 야기할 수 있는 단점은 상속시에 일반화(generalization)의 개념을 허용할 수 없다는 결과가 된다. 왜냐하면 정보 보안환경에서, 객체의 기밀성이 특성화에서 일반화로 변화됨에 따라서 더 낮은 비밀등급이 부여될 수 있기 때문이다. 그리고 [Mill92]의 경우에서도 보안성 유지를 위하여 어떤 객체의 상속은 상속된 객체의 비밀등급은 상속을 제기한 객체의 비밀등급과 같이 상속을 원칙으로 한다. 이러한 경우에 단점은 정보 보안 모델이 어렵고, 융통성이 없으므로 약한 정보 보안 모델을 가질 수 있다. 그러나 본 논문에서 제시하는 질의관리의 참조 제한기법은 무제한 상속을 허용하기 때문에 풍부한 데이타 모델을 가질 수 있을 뿐만 아니라, 더욱 견고한 정보 보안 모델과 융통성 있는 데이타베이스 모델을 표현할 수 있기 때문에 기존에 다른 연구결과와 구별된다.

2. 관련연구

1.2 보안정책

일반적으로 보안정책을 기술하기 위하여는 객체와 주체라는 용어를 이용하여 보안정책의 운영규약을 정의한다. 객체는 데이타 화일, 레코드 또는 레코드내의 필드로 이해될 수 있으며, 주체는 객체들에 대한 접근을 요청할 수 있는 활성화된 프로세스, 혹은 사용자를 말한다. 어떤 특정 주체에 의하여 객체의 접근제어를 위한 보안정책은 크게 임의적 접근제어(discretionary access control: DAC) 정책과 강제적 접근제어(mandatory access control: MAC)[Sand 90]정책으로 구분할 수 있다. DAC정책은 주체나 그의 주체가 속해 있는 그룹의 식별자를 근거로 하여 객체에 대한 접근을 제한하는 방법이다. MAC은 이에 반하여 객체에 포함된 정보의 비밀등급과 주체에 부여된 비밀취급인가 등급을 기반으로 하여 객체에 대한 접근을 제어하는 방법이다. MAC정책은 다단계 보안(multi-level security: MLS) 기법 구현을 위한 방법론적 핵심이 되며 다단계 보안기법을 기반으로 하여 구축된 데이타베이스 시스템을 다단계 보안 데이타베이스 체계[Keef 90]라고 한다.

대부분의 상용 데이타베이스 관리 시스템들이 채택하고 있는 보안 유지 방법은 데이타에 대한 사용자들의 사용권한 여부에 관한 제한을 데이타 생성자 의도에 따라 하는 것을 허용하는 임의적 접근제어 방식에 기반을 두고 있다. 임의적 접근제어 방식이라고 명명된 이유는 데이타에 대한 사용권한을 다른 사용자들에게 임의대로 넘겨주는 것이 허용되는 접근제어 방식이기 때문이다. 이러한 DAC 방식은 대부분의 정직한 그리고 인증된 사용자들을 통한 정보의 유출을 방지하는 경우에는 적합할 수 있으나, 악의적인 침입자들의 트로이 목마를 이용한 데이타의 접근 또는 컴퓨터 바이러스에 의한 데이타의 접근은 반드시 제한되고 방지되어야 함에도 불구하고 원천적으로 방지할 수 없다는 결함을 가지고 있다. 트로이 목마란 인가된 이용자에 의해 수행되어지는 프로그램의 내부에 삽입이 되어 악의적으로 정보를 유출시키는 코드를 말한다.

DAC의 이러한 결점을 극복하기 위한 대안이 강제적 접근제어 방식이다. MAC 방식의 운영은 일반적으로 Bell-LaPadula 모델[Lunt90]에 기초를 두고 있다. MAC 정책 운영 환경하에서는 모든 객체는 비밀등급이 할당되며, 모든 주체도 취급이 인가된 등급별 비밀등급이 부여된다. 객체와 주체에 부여된 비밀등급을 바탕으로 하여 Bell-LaPadula 모델은 아래의 제약조건을 MAC 정책의 운영에 적용한다.

- **상향판독 금지 특성(simple security property)**: 주체의 비밀등급이 객체의 비밀등급보다 낮은 경우에는 객체에 대한 주체의 판독이 금지된다.
- **하향갱신 금지 특성(* -Property)**: 주체의 비밀등급이 객체의 비밀등급보다 높은 경우에는 객체에 대한 갱신이 금지된다.

Bell-LaPadula 모델에서 제시하고 있는 두 가지 제약조건을 준수하여 MAC 정책이 운영된다면 데이타를 접근하는 과정에서는 상위 비밀취급 인가자로부터 하위 비밀취급 인가자로의 정보의 직접적인 유출은 방지됨이 보장되어 진다. 이러한 제약조건들은 OODBS의 질의 보안 기능을 통하여 모든 판독과 갱신연산에 대하여 자동적으로 적용되기 때문에 트로이 목마에 의한 정보의 누설을 점검하고 방지할 수 있다.

2.2 객체 보안모델

다단계 보안 객체지향 데이타베이스 시스템에서 모든 개념적인 개체는 기밀성의 정도에 따라서 비밀등급이 부여된 객체들로 표현된다. 이렇게 표현된 객체는 정적인 상태를 표시하기 위한 속성의 집합과, 그의 행위를 표시하기 위한 방법의 집합으로 구성된다. 이때 그 객체를 구성하고 있는 속성에 대한 값은 그의 기밀성에 따라서 비밀등급으로 분류되어 저장된다. 본 논문에서는 이러한 개념을 보안 객체모델(secure-object model: SO-Model)이라고 한다. 여기서 객체의 비밀등급의 결정은 다음과 같이 Bell-LaPadula의 모델에 따른다.

정의1 (등급함수): 객체의 집합을 O라고 하고, 주체의 집합을 S라고 한다. 그리고 보안 분류의 집합을 L이라고 할 경우 등급 사상 함수를 f라고 할 경우에 다음과 같은 식이 유도된다.

$$f : O \cup S \rightarrow L$$

만일 어떤 객체 o_1, $o_2 \in O$에서 역함수 $L(o_1)$이 $L(o_2)$를 지배할 수 있을 경우에는 객체 o_1은 o_2의 비밀등급 보다 높게 분류되었다고 한다. 예를 들면 군의 보안 분류에서 비밀등급 최상위 보안(top security: TS)〉보안(security: S)〉3급비밀(confidential: C)〉대외비(unclassified: U)라면 MLS/OODB에 보관되어 있는 어떤 객체 o는 이들 중에 하나로 결정된다.

다단계 보안 객체지향 데이타베이스에서 어떤 객체는 객체의 식별자(다른 객체와 유일하게 구별되는 식별값)와 객체의 속성 값이 보안 분류 대상이 된다. 따라서 보안 객체의 표현은 다음과 같다.

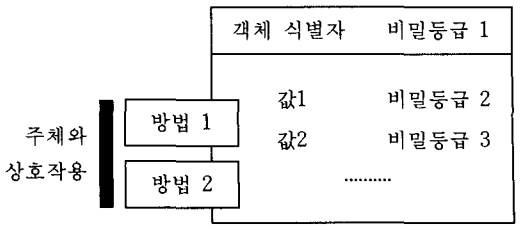

그림 2.1 보안 객체의 표현

이러한 보안 객체들은 객체를 생성하는 틀로 사용되는 보안 분류된 부류로 부터 생성된다.

이러한 부류의 유형은 시스템에 의해서 묵시적으로 정의된 것과, 사용자의 의해서 명시적으로 정의되는 것으로 나를 수 있다.

정의2 (시스템 부류의 보안분류): 시스템에 의해서 정의된 부류 객체의 비밀등급은 보안 분류의 범주중에서 가장 낮은 비밀등급을 가진다.

예를들면 정수형, 문자형, 실수형과 같은 무결성을 보장하기 위하여 정의되는 시스템 부류와 객체지향 데이타베이스의 최상위 부류 객체는 보안 분류중에서 가장 낮은 보안 분류를 가진다.

이러한 것은 시스템의 효율적 접근을 보장하기 위함이다.

정의3 (속성의 보안 성질): 어떤 보안 객체 O와, 그의 속성 V는 다음과 같은 보안 분류 관계가 만족 되어야 한다.

$$L(V) \geq L(O)$$

정의 3은 부류 객체의 비밀등급 보다 속성의 비밀등급이 낮으면 이러한 속성의 값은 접근할 수 없게 된다. 예를 들면 3급 비밀로 분류된 부류의 이름 '고객'의 속성 '주소'와 '전화번호'는 3급 비밀로 분류되었고, 또 다른

속성 '급여액'은 2급 비밀로 분류할 수 있다. 그러면 3급 비밀취급 인가 등급을 가진 사용자는 '급여액'의 값은 읽을 수 없게 된다. 따라서 객체와 그 객체의 값의 비밀등급은 부류와 그 부류의 속성에 부여된 비밀등급에 의하여 결정된다.

데이타베이스 사용자는 전문전달을 통하여 부류의 방법을 호출하여 보안 객체를 접근할 수 있다. 객체지향 시스템에서 행위에 융통성을 부여하기 위하여 방법은 비보안으로 분류한다. 그러나 방법을 호출하기 위한 전문은 보안 분류를 가진 가진다. 즉, 전문은 데이타베이스를 사용하는 주체에게 부여된 비밀 취급인가 등급과 같다. 만일에 주체 S가 3급으로 보안 분류되었다면 L(S) = C(classified)가 성립한다고 한다. 예를 들면, 비밀등급 C로 '고객' 부류 객체로 생성된 객체의 이름을 '홍길동'라고 하자. 그리고 그의 값은 다음 그림 2.2와 같다고 가정한다.

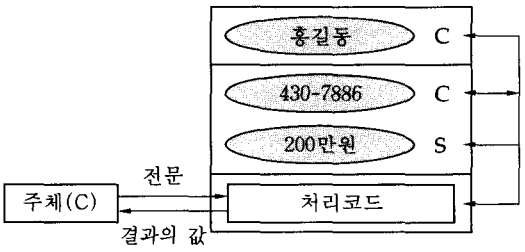

그림 2.2 보안 객체의 접근에 대한 예

그림 2.2에서 3급 비밀 취급인가가 부여된 사용자는 전문을 통하여 '홍길동' 객체를 접근하려고할 때에 전문도 역시 3급 비밀로 분류되어 전달되게 된다. 그 결과 고객의 성명 '홍길동'과 그의 전화번호 '430-7886' 값은 읽을 수 있지만 고객의 수입은 읽을 수 없다. 이러한 전문의 유형은 보안 객체의 값을 읽기 위한 것과, 그 객체의 값을 갱신하기 위한 것으로 나눌 수 있다.

보안 객체의 값을 판독하기 위한 전문 유형과 갱신하기 위한 유형은 다음과 같다.

(1) 판독: method mane(object_id, value, boolean)

(2) 갱신: method_mane(object_id, value)

본 논문에서 방법은 비보안이다. 그러나 방법을 수행하기 위해서는 전문의 전달을 통해서 이루어 지는데, 전문은 비밀등급을 가지고 있다. 이러한 전문의 비밀등급은 다음과 같다.

정의4 (전문의 보안 분류): 어떤 주체 S가 전문 m을 통하여 방법의 집합 M을 수행한다고 하자. 그러면 이들의 비밀등급은 다음과 같다.

$$L(S) = L(m) = L(M)$$

이 성립한다.

2.2 부류 객체의 상속

보안 객체모델은 부류의 계층구조를 포함한다. 왜냐하면 이러한 부류의 계층구조는 데이타베이스내에 중복된 보안 객체의 수를 줄이고 데이타의 일관성을 유지할 수 있는 장점이 있기 때문이다. 이러한 부류의 계층구조는 일반화, 특성화에 관련된 (is-a)계층구조와 구성, 통합(aggregation)에 관련된 부품(is-part-of) 계층구조[Grah94]로 분류된다. 이러한 부류 계층구조는 데이타베이스의 보안 객체들의 의미에 따라서 나누어 지게 된다.

부류의 계층구조는 상위 부류와 하위 부류의 구조로 설계된다. 이때에 하위 부류는 상위의 부류의 속성과 방법을 상속받게 된다. 예를 들면 부류 '고객'와 '근로자'는 부류 '회사'의 하위 부류이다. 그리고 부류 '경영자'와 '사무원'은 부류 '근로자'의 하위 부류이다.

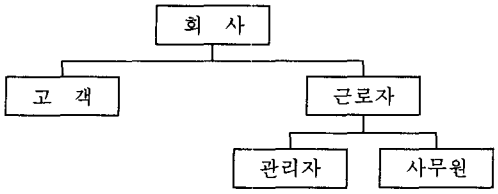

그림 2.3 종류형의 부류 계층구조

다른 한편으로 부품 부류 구조는 구성 객체들을 기술하는데 사용한다. 여기서 구성 객체들은 다른 객체의 부품이 된다. 예를 들면 부류 '회사'는 부류 '근로자', '설비', 그리고 '자본'로 구성된다.

그림 2.4 부품형의 부류 계층구조

하위 부류는 상위 부류의 특성화되거나 구체화된다. 여기서 하위 부류의 비밀등급은 상위 부류의 비밀등급을 지배해야한다. 이러한 것을 다음과 같이 정의한다.

정의5 (부류 계층구조의 비밀등급): 두개의 부류 객체를 O_1과 O_2라고, O_1는 O_2의 상위 부류 라고 한다면 다음과 같은 관계를 가져야 한다.

$$L(O_2) \geq L(O_1)$$

정의 5는 정보의 상향 이동을 막기 위하여 필요한 제한 사항으로서 정의된다. 왜냐하면 부류의 계층에서 하위 부류의 접근은 그의 상위 부류의 접근을 허락할 수 있기 때문이다.

3. 객체 보안 운영

3.1 상속에 관한 보안문제

다단계 보안 객체지향 데이타베이스는 현실세계의 객체들을 자연스럽게 모델링할 수 있을 뿐만 아니라 MAC을 기초로 하는 견고한 보안 시스템을 구축할 수 있다. 이는 앞 절에서도 언급하였듯이 객체의 표현 과정에서의 정보은닉 수단을 객체지향 시스템이 지니고 있기 때문이다. 즉, 사용자가 데이타 객체의 값들을 접근하기 위해서는 방법과의 상호작용을 통해서만 가능하다. 그러나 객체간의 상속이 요구되는 경우에 보안 문제를 해결한다는 것은 난제로 남아 있다. 왜냐하면 상속의 수단은 객체와 객체 사이의 가시성(visibility)을 증가시키는 결과를 초래함으로서 정보의 은닉성(encapsulation)의 감소와 결부되기 때문이다.

부류 계층구조에서 상속에 관련된 보안 위반에 관한 경우를 살펴보면 그림 3.1과 같다. 부류 B는 부류 A의 하위 부류이고, 부류 B는 부류 A의 속성 값 V을 상속 받았다고 가정한다.

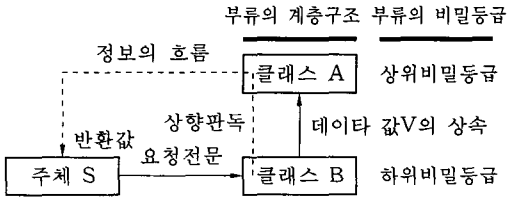

그림 3.1 하위 부류로 부터의 상속

또한, 부류 B는 하위 비밀등급으로 분류된 객체이고, 부류 A는 상위 비밀등급으로 분류된 객체라고 가정한다. 부류 B와 동등한 비밀취급인가 등급을 가진 주체 S가 객체 부류 B를 접근하려고 할 때에, 주체 S는 부류 B가

클레스 A로 부터 상속받고 있는 데이타 V를 접근하는 것이 허용됨에 따라 결과적으로 부류 A의 데이타 값에 대한 접근을 허용받게 된다. 이러한 경우 주체 S의 비밀취급인가 등급이 부류 A의 비밀등급보다 낮음에 따라 Bell-LaPadula의 상향판독 금지 특성을 위반하게 된다.

이러한 위반사항을 해결하기 위하여 그림 3.2와 같이 부류 B의 비밀등급이 부류 A의 비밀등급 보다 높은 경우를 가정한다.

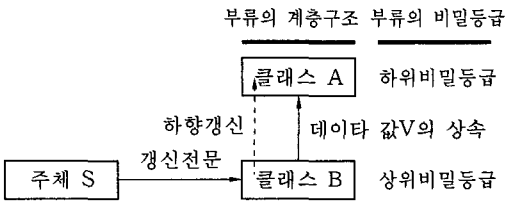

그림 3.2 상위 부류로 부터의 상속

만약, 부류 B와 동일한 비밀등급을 가지고 있는 상위 비밀 취급인가자 S가 부류 B의 속성값 V를 갱신하려고 한다면 부류 B로부터 하위의 비밀등급으로 분류된 부류 A의 데이타 값에 대한 갱신이 발생하게 된다. 이 경우 주체 S의 비밀 취급인가등급이 부류 A의 비밀등급보다 높기 때문에 Bell-LaPadula 모델의 이러한 갱신 시도는 하향 갱신 금지 특성을 위반하게 된다.

3.2 보안 객체모델의 제약조건

데이타의 제약은 데이타베이스의 정확성과 보안성을 보장하기 위한 중요한 개념이다. 다단계 보안 객체지향 데이타베이스 시스템에서 이러한 제약조건은 무결성 제약조건과 비밀등급 제약조건으로 나뉠 수 있다. 무결성 제약조건은 객체의 변수가 표현할 수 있는 값의 범위를 제한하는 것으로서 사용자에 의하여 정의된다. 그리고 비밀등급 제약조건은 객체에게 가능한 비밀등급을 제약하는 것으로서 역시 보안 통제자에 의하여 부여된다.

다단계 보안 객체지향 시스템에서 제약조건은 객체에 속한 속성의 값이 참조될 때에 자동적으로 호출되는 방법에 의하여 이루어진다. 이러한 제약은 어떤 객체에서 혹은 그 객체가 참조(상위의 객체)하고 있는 객체의 방법에 의해서 제한하게 된다. 이러한 방법에는 객체값의 정확성을 보장하기 위한 제약조건을 부과(가령, 정수형, 실수형, 문자형 등)해야할 뿐만아니라 그의 값의 비밀등급 제약조건을 같이 포함되어야 한다. 가령 대외비로 분류된 객체 'CUSTOMER'의 변수 'income'은 2급 비밀로 분류되어 있다면 다음과 같은 구문으로 표시해야 한다.

```
class CUSTOMER<classification: U>
return(income.level = S);
```

만일 부류 계층구조에서 어떤 객체는 상위의 객체로 부터 상속 되었다면 이 객체는 상위의 객체의 값을 참조할 경우가 있다. 이러한 경우에도 데이타 값의 정확성을 보장할 수 있어야 하지만 Bell-LaPadula 보안 성질을 위배하지 말아야 한다. 따라서 다음 구문과 같이 객체의 참조시에 비밀등급의 제약조건을 부과해야 된다.

```
class CUSTOMER<classification: U>
reference(COMPANY.incom.level = S);
```

본 논문에서는 제 4장에서 MLS/OODB의 참조제약 기법을 이용한 접근제어 규약에 대하여 살펴본다.

3.2 상속 문제 해결에 관한 기술 동향

객체지향 데이타베이스의 상속시에 보안성 확보를 위한 선행 연구[Lunt90, Mill92, Morg92]들에서는 부류 상속시에 제약을 부여하는 방식을 적용하고 있다. [Lunt90]과 [Morg92]는 상위 부류 객체의 비밀등급이 하위 부류 객체의 비밀등급 보다 높은 경우에 이들 부류간의 상속을 제한하고 있다. 이러한 상속상의 제한은 상향 판독(주체의 비밀등급 보다 높은 객체의 판독)이나 하향 갱신(주체의 비밀등급 보다 더 낮은 객체의 값을 갱신)을 통한 상위 비밀등급의 객체로부터 하위 비밀등급 객체로의 정보 흐름을 차단하는데 목적이 있다. 이러한 상속의 제한에 따른 문제점은 상속시에 일반화(generalization)의 개념을 허용할 수 없다는 결과가 된다. 왜냐하면 정보 보안 환경에서, 객체의 비밀성이 특성화에서 일반화로 변화됨에 따라서 더 낮은 비밀등급이 부여될 경우도 있지만 이러한 것을 허용하지 않으므로서 데이타 객체 모델의 문제를 가질 수 있기 때문이다. 그리고 [Mill92]는 부류 객체들간의 상속은 이들 부류들의 비밀등급이 동일한 경우에만 허용하는 방법을 채택하고 있다. 서로 다른 비밀등급을 가지는 부류간에서의 상속을 제한하는 이러한 기법은 필연적으로 데이타 모델링을 하는 과정에서 데이타 표현상의 융통성을 감소시킬 것이다.

객체를 접근하는 과정에서의 보안성을 얻기 위한 이러한 선행 연구 기법들은 객체지향 모델이 가지는 강력한 표현 방법인 상속성질에 제약을 부가하는데 그 방법적 기반을 두고 있다. 이러한 상속성질의 제한은 데이타 모델링 과정에서의 표현 능력에 제약을 초래하고, 이러한 제약을 극복하는 과정에서 구축될 데이타베이스의 중복된 의미의 객체가 존재하도록 허용하게 된다.

이러한 중복성의 허용은 데이타 중복성을 최대한 제한하고자 하는 데이타베이스 시스템 본연의 취지를 벗어나게 된다.

4. 질의 보안 관리

데이타 접근에 대한 보안성을 검증하는 방법은 크게 보수적 관점에서의 보안 검증과 낙관적 관점에서의 보안 검증으로 구분할 수 있다. 보수적인 보안 검증 방법은 데이타에 대한 주체의 접근이 제기되기 전에 발생 가능한 모든 종류의 보안 위반의 경우를 구조적으로 차단하는 방법이다. 이에 반하여, 낙관적인 검증 기법은 주체가 제기한 데이타에 대한 접근이 발생하는 시점에서 비로소 보안 검증이 이루어지도록 하는 방법이다. 보안성을 유지하면서 상속 문제를 해결하기 위한 선행 기법들은 보수적인 관점에서 접근하고 있다. 이는 2.2에서도 언급한 데이타 모델링 과정에서의 표현상의 융통성에 제약이 따르게 된다. 이러한 제약사항들을 개선하기 위하여 본 논문에 질의 보안 관리기는 다음과 같은 개념을 고려하였다.

(1) 데이타 모델링 과정에서의 상속에 대한 요구를 제약없이 수용한다.
(2) 데이타 모델링의 결과에 따라 구축된 데이타를 어떤 주체가 접근하는 시점에서 보안 검증을 실시하는 낙관적인 기법을 채택한다.

상속에 대한 요구를 제약없이 수용하기 위해서는 객체의 보안등급에 대한 고려를 제외하여야 한다. 객체의 보안등급에 대한 고려의 제거는 데이타 모델링에서 제시한 상속의 요구을 반영하는 과정에서의 보안성에 대한 고려에 융통성을 부여하게 된다. 보안성에 대한 이러한 융통성의 부여는 보안성에 대한 검증을 주체가 제기한 방법이 객체의 데이타를 접근하는 싯점으로 지연시키는 낙관적인 보안검증 기법을 채택하도록 유도하게 된다. 따라서

이러한 방법론은 객체의 상속에 대한 보안상의 모든 제한사항들을 해소할 수 있게 한다.

이에 따라 주체가 제기한 방법과 그 방법이 접근하게 되는 데이타가 보안성 검증의 대상이 된다. 데이타베이스를 사용하는 주체는 전문의 형태로 방법을 호출한다. 따라서 데이타를 접근하게 되는 방법의 비밀등급은 그를 근본적으로 호출한 주체의 비밀등급과 동일한 비밀등급을 부여 받게 된다. 이렇게 호출된 방법은 데이타를 판독하고 갱신하는 연산들의 집합과 이들 연산들이 접근하는 데이타들을 처리하는 연산들의 집합으로 이루어지게 된다. 방법의 수행과정에서 실행되는 이러한 모든 판독 혹은 갱신 연산들이 데이타를 접근하는 과정에서 컴퓨터 시스템에서 채택하고 있는 보안정책을 위반하지 않음이 검증되는 경우에만 방법은 성공적으로 수행되며 이들중 보안성을 위반하는 연산이 제기되었을 경우에는 방법의 수행은 거절된다.

방법이 데이타를 접근하는 과정에서 요구되는 이러한 규약을 수행하기 위하여는 다음과 같은 정의들을 필요로 한다.

■ 정의 6 (판독/갱신 데이타 집합):

- R(m)은 전문 m이 판독을 위해 접근하는 데이타들의 집합.
- W(m)은 전문 m이 갱신을 위해 접근하는 데이타들의 집합. n

■ 정의 7 (판독/갱신 데이타 보안 등급):

- L(R(m))은 R(m)을 구성하고 있는 데이타들의 보안 등급들중 최상의 보안등급.
- L(W(m))은 W(m)을 구성하고 있는 데이타들의 보안 등급들중 최하의 보안등급.
- L(m)은 전문 m의 보안등급. n

◈ 정리 1 (상향판독금지 검증 규약):

전문 m이 상향 판독금지 특성을 위반하지 않도록 하기 위해서는 다음과 같은 제한사항을 준수하여야 한다.

(1) $W(m) = \{\emptyset\}$ 이고 $L(R(m)) \leq L(m)$인 경우에는 방법 M의 수행을 허용

(2) $R(m) \neq \{\emptyset\}$ 이고 $L(R(m)) > L(m)$인 경우에는 방법 M의 수행을 거부.

증 명: 어떤 주체 S가 전문 m을 통하여 특정 객체의 값을 접근하려고 한다. 그러면 정의 4에 의하여 $L(S) = L(m)$이 성립된다. 이때 m의 판독연산의 집합 $R(m) = \{x, z\}$, 이고 기록연산 $W(m) = \{\emptyset\}$이라고 한다.

한편 두개의 객체 O_1, $O_2 \in O$가 존재하고 O_2는 O_1으로 부터 모든 속성을 상속 받았다고 하자. 이를 $O_1 \leftarrow O_2$으로 표기한다. 그리고 O_1의 속성의 집합 $A_1 = \{x, y\}$이고 O_2의 속성의 집합 $A_2 = \{A_1, z\}$라고 한다. 그러면 R(m)은 당연히 A_2에 속한다. 이때 $L(R(m) \cap A_2)$의 최대 비밀등급을 L_1이라고 할 경우에 문제에 의하여 (1)의 경우는 $L(m) \geq L_1$이므로 Bell-LaPadula의 상향판독 금지 특성에 위배되지 않는다. 따라서 판독을 위한 방법 M의 수행을 허락한다. 그리고 두번째 경우는 이러한 증명의 역의 관계가 성립 됨으로서 Bell-LaPadula의 상향판독 금지특성을 위배된다.

◈ 정리 2 (하향갱신금지 검증 규약):

전문 m이 하향갱신금지 특성을 위반하지 않도록 하기 위해서는 다음과 같은 제한사항을 준수하여야 한다.

(1) $R(m) = \{\emptyset\}$ 이고 $L(W(m)) \geq L(m)$인 경우에는 방법 M의 수행을 허용.

(2) $W(m) \neq \{\emptyset\}$ 이고 $L(W(m)) < L(m)$인 경우에는 방법 M의 수행을 거부.

증 명: 정리 1에서 와같이 어떤 주체 S가 전문 m을 통하여 특정 객체의 값을 접근하려고 한다. 그러면 정의 4에 의하여 $L(S) = L(m)$이 성립된다. 이때 m의 판독연산의 집합 $R(m) = \{\emptyset\}$ 이고 기록연산 $W(m) = \{x, z\}$이라고 한다.

한편 두개의 객체 O_1, $O_2 \in O$가 존재하고 O_2는 O_1으로 부터 모든 속성을 상속받았다고 하자. 이를 $O_1 \leftarrow O_2$으로 표기한다. 그리고 O_1의 속성의 집합 $A_1 = \{x, y\}$이고 O2의 속성의 집합 $A_2 = \{A_1, z\}$라고 한다. 그러면 R(m)은 당연히 A_2에 속한다. 이때 $L(R(m) \cap A_2)$의 최대 비밀등급을 L_1이라고 할 경우에 문제에 의하여 (1)의 경우는 $L_1 \geq W(m)$ 이므로 Bell-LaPadula의 하향 갱신 금지특성(* -property)을 위배하지 않는다. 따라서 갱신을 위한 방법 M의 수행을 허락한다. 그리고 두번째 경우는 이러한 증명의 역의 관계가 성립됨으로서 Bell-LaPadula의 하향 갱신 금지특성(* -property) 금지특성을 위배된다.

방법의 데이타 접근은 항상 상향판독 금지검증과 하향갱신 금지검증을 거친 후 이루어 지게 되며 이러한 검증을 거친 방법의 수행은 Bell-LaPadula 모델에 근간을 두고 있는 보안정책을 준수함이 보장된다. MLS/OODBMS에서의 질의 보안 관리기는 이러한 검증이 보안성을 요구하는 모든 데이타 객체 및 방법에 자동적으로 상기 규약의 보안검증을 거치게 된다.

5. 결 론

보안성 질의관리는 객체지향 시스템을 기반으로 하여 구축되어지는 정보 시스템이 보안정책의 요구사항을 성공적으로 유지하는데 있다. 이를 위해서 본 논문에서는 객체지향 모델이 가지고 있는 데이타 표현력에 손상을 주지 않은체 보안성을 최대한으로 유지하도록 하는데 역점을 두고 수행하였다. 이를 위하여 무제한의 상속모델을 허용하고 보안성 확보는 질의 처리시에 참조제약 기법을 통하여 수행함으로서 낙관적인 보안성 확보에 배려를 했다. 그러나 이러한 객체지향 데이타베이스 시스템이 모델시에 보안성의 측면을 고려하여 설계하는 것이 아니고 질의 처리시에 보안성 검증을 수행하기 때문에 검증에 필요한 시스템에 부담을 가져올 수 있다. 그렇지만 데이타베이스의 보관된 객체들 자체는 보안의 문제가 되는 것이 아니라 이들이 활성화될 경우에 보안성의 문제를 발생할 수 있기 때문에 객체의 활성화 최초 단계인 질의관리기에 의해서 담당하게 하는 것이 타당하다고 사료된다. 이러한 장점은 객체지향 데이타베이스의 모델에 보안성을 부여로 인하여 과도한 모델 구성의 제약사항을 감소시킴으로서 풍부한 객체모델을 가질 수 있다는 것이다. 그리고 질의처리시에 보안성 검증을 수행하기 때문에 보안관리에 융통성을 부여할 수 있다는 장점도 가지고 있다.

그러나 질의 관리에서 직접적인 정보의 유출을 방지시킬 수 있음에도 불구하고 다단계 보안 OODBMS에서 데이타베이스의 정확성을 보장하기 위하여 동시에 객체를 접근하려고 하는 거래들의 동시성을 제어하게 되는데, 이러한 과정에서 간접적인 정보의 유출이 발생할 수 있는 통로가 형성될 수 있다. 이와 같은 간접적인 정보의 유출 통로를 비밀경로(covert channel)라고 한다. 이러한 비밀경로의 형성은 공유자원의 접근여부를 탐지하거나 데이타베이스의 응답시간의 차이를 탐지하는 과정에서 발생할 수 있다. 이러한 문제는 거래들의 동시성 제어시에 발생하기 때문에 본 논문의 연구범위에서 제외하였다. 따라서 우리는 객체지향 데이타베이스 관리체계에서 비밀경로의 문제를 해결하기 위한 보안 동시성제어 기법에 대하여 계속적인 연구를 수행하고 있다.

참 고 문 헌

[Grah 94] Lan Graham, Object-Oriented Methods 2nd Ed., Addison-Welsley Publishers Ltd., ISBN 0-201-59371-8, 1994.

[Keef90] T. F. Keefe, W. T. Tsai and J. Srivastava, "Multilevel Secure Database Concurrency Control," Proceedings of IEEE Symposium on Security and Privacy, 1990, pp. 337 - 344.

[Lunt89] Teresa F. Lunt,, "Access Control Policies for Database Systems," DATABASE SECURITY, II: Status and Prospects, ed. C.E. Landwehr, Elsevier Science Publishers B.V., 1989, pp. 41-52.

[Lunt90] Teresa F. Lunt, "Multilevel Security for Object-Oriented Database Systems," Database Security III: Status and Prospects, ed. D.L Spooner and C. Landwehr, Elsevier Science Publishers B.V., 1990, pp.199-209.

[Mill92] J. K. Millen and Teresa F. Lunt, "Security for Object-Oriented Database Systems," Proceedings of the IEEE Symposium on Security and Privacy, Oackland, CA, 1992, pp260-272.

[Morg91] Dr. Matthew Morgenstern, "A Security Model for Multilevel Object with Bidirectional Relationships," DATABASE SECURITY II: Status and Prospects, C.E, Landwehr(Editor), IFIP, 1991, pp. 53-71

[Sand90] Ravi Sandhu, "Mandatory Controls for Database Integrity," DATABASE SECURITY III: Status and Prospects, ed. David L. Spooner, Carl Landwehr, Elsevier Science Publishers B.V., 1990, pp. 143 - 150.

□ 著者紹介

최 용 구(崔 溶 龜)

1984년 서원대학교 사범대학 수학과 학사
1990년 중앙대학교 국제경영대학원 경영정보학과 석사
1995년 한국과학기술원 정보 및 통신공학과 컴퓨터공학 전공 석사
1995년 3월~현재 한국과학기술원 정보 및 통신 공학과 컴퓨터공학 전공 박사과정중
1989년 9월~ 1992년 2월 한국전력공사 서울연수원 전산교수실
1992년 3월~현재 대유공업전문대학 사무자동화과 전임강사, 조교수
※ 관심 분야: 객체지향 데이타베이스, 데이타베이스 보안, 동시성제어

문 송 천(文 松 天)

1975년 숭전대학교 전산학과 학사
1977년 한국과학기술원 전산학과 석사
1985년 University of Illinois at Urbana-Champaign 전산학과 박사
1977년 3월~ 1985년 4월 숭전대학교 전산학과 조교수
1981년 9월~ 1984년 8월 미국육군연구소(CERL)연구원
1985년~현재 한국과학기술원 교수
1989년, 1994년 영국 에딘버러대학, 캠브리지대학 객원교수
1990년~1992년 한국정보과학회 데이타베이스 연구회 회장
1991년 미국정보과학회(ACM) DB연구회 학술위원
1991년 4월~1993년 4월 DASFAA93 국제학술대회 학술의장
1991년 9월~현재 유럽정보과학회(EUROMICRO)상임이사
1991년, 1995년 니카라과정부 외무부 자문역, 루미니아정부 산업부 자문역
1994년 헝가리 과학원 초청 저명과학자
1994년 10월 한국정보과학회 이사