

# 객체지향 데이터베이스에서 다중상속에 대한 보안속성 확장†

조기천\*<sup>0</sup> 신문선\* 김은희\* 류근호\* 김명은\*\*

\*충북대학교 데이터베이스연구실

\*\*한국전자통신연구원

e-mail:\*(kicheon, msshin, ehkim, khryu)@dblab.chungbuk.ac.kr

\*\*mekim@etri.re.kr

## The Expansion of Security property on the Multiple Inheritance in the Object-Oriented Databases

Ki-Cheon Cho\*<sup>0</sup>, Moon-Sun Shin\*, Eun-Hee Kim\*, Keun-Ho Ryu\*, Myung Eun Kim\*\*

\*Database Laboratory, Chungbuk National University

\*\*ETRI

### 요 약

객체지향 데이터베이스의 보안모델에서 사용되는 보안정책과 보안속성들은 새로운 보안 모델이 제시될 때마다 그 개념과 적용범위가 다르게 정의되어왔다. 객체지향 데이터베이스는 객체지향 시스템의 특징과 데이터베이스의 특징들을 만족해야 하는데, 객체지향 시스템의 중요한 요소 중의 하나인 상속 계층에 대해서 많은 연구가 진행되어왔다. 기존의 객체지향 데이터베이스 시스템 대부분은 슈퍼클래스와 서브클래스 사이의 단일상속만을 고려하였거나 또는 다중상속을 전혀 고려하지 않았다. 이로 인해, 클래스 사이의 다중상속을 정의할 경우 시스템을 설계할 때 만족되어야 하는 보안속성의 위배가 일어날 수 있는 문제점이 있다. 따라서, 이 논문에서는 클래스 계층 사이의 다중상속을 정의할 때 기본적으로 충족되어야 하는 보안속성에 대한 추가적인 정의를 제시한다.

### 1. 서 론

객체지향 데이터베이스에서의 보안 목적은 일반적인 데이터베이스와 마찬가지로 데이터베이스에 대한 권한이 없는 사용자의 액세스를 제어하여 정보의 고의적인 파괴 또는 변경 등을 방지하고, 우발적으로 발생할 수 있는 사고로부터 데이터를 보호하는 것이다. 데이터베이스는 일반적으로 대용량의 자료를 보관하기 때문에 데이터의 무결성(Integrity), 기밀성(Secrecy), 가용성(Availability)의 보장이 필수적으로 요구된다[6,7].

객체지향 데이터베이스 시스템에 대한 보안 연구는 임의 보안 정책과 강제 보안 정책을 적용해서 이루어졌으며, 임의 보안 정책을 적용한 모델로는 대표적으로 ORION 모델이 있고, 강제 보안 정책에는 Millen-Lunt 모델이 있다[4]. ORION 모델에서는 다중상속을 허용하지만 권한을 가진 사용자가 임의적으로 다른 사용자에게 자신의 권한을 부여하거나 철회할 수 있는 임의 보안 정책의 단점을 가지고 있다. 따라서, 강제 보안 정책을 적용한 모델들을 많이 개발해 왔다. 이러한 모델 중에 Millen-Lunt 모델이 많이 적용됐지만, 이 모델에는 객체지향 모델링에서 가장 중요한 개념인 상속계층 구조에서의 다중 상속에 대한 연구가 거의 이루어지지 않았다 [1,2,3].

이 논문에서는 객체지향 데이터베이스의 다중상속 개념과 기존의 객체지향 데이터베이스에서 클래스간의 또는,

클래스의 애트리뷰트나 메소드 사이에 만족되어야 하는 보안속성에 대해서 기술한다. 그리고, 다중상속에 대한 보안속성과 다른 모델에서 제시되지 않았던 다중상속에 따른 문제점을 제시하고 이를 해결하기 위해서 새로운 보안속성을 제안한다.

### 2. 객체지향 데이터베이스 시스템

#### 2.1. 다중상속

클래스 계층 구조에서 다중상속은 하위 클래스가 하나 이상의 상위 클래스로부터 애트리뷰트와 메소드를 상속 받는 것을 의미한다.

초기 객체지향 언어인 Smalltalk의 상속구조는 하나의 하위 클래스에 단지 하나의 상위 클래스로 제한되었으며, 트리 형태의 계층적인 구조로 표현되었다[5].

하지만, 현재의 객체지향 시스템에서는 대부분 하나 이상의 상위 클래스를 가질 수 있도록 정의하고 있다. 다중상속의 경우 계층구조는 일반적으로 격자 구조로 표현한다.

다중상속에는 여러 개의 상위 클래스로부터 애트리뷰트와 메소드를 상속받기 때문에 다음과 같은 문제가 발생할 수 있다. 클래스 Engineer와 Manager의 하위 클래스로서 Engineering\_Manager를 생성한다고 가정하자. 만약 Engineer와 Manager 모두 Salary라는 메소드를 가지고 있다면, 하위 클래스는 Salary라는 메소드를 Engineer와 Manager 중에서 어느 상위 클래스의 메소드를 사용할 것인지 결정을 해야만 한다. 또한, Engineer와 Manager는 단지 Engineering\_Manager의 상위 클래스일 뿐 다른 상위 클래스(예를 들면, Employee와 같은)에서

† 이 연구는 2001년도 한국전자통신연구원의 네트워크 보안구조 연구팀의 위탁과제 연구에 의해 수행됨

Salary 메소드를 상속받았을 수도 있다.

이러한 두 가지의 경우에 하나의 해법은 하위 클래스에 상속되는 메소드들이 상속계층에서 어느 상위 클래스의 메소드를 상속받게 될 것인지 우선 순위 규칙(priori rule)을 사용하거나, ORION 모델에서와 같이 Engineer와 Employee의 상위 클래스를 생성하는 방법이 있다.

**2.2. 보안속성**

객체지향 데이터베이스 보안모델의 상속에 대한 일반적인 보안속성들을 다음과 같다[2,3,5,7].

우선 상속에 대한 속성을 알아보기 전에 속성 정의에 쓰이는 함수를 정의한다.

• 보안등급부여함수(CGF:Classification Grant Function)  
 $CGF(X_1, X_2, X_3, \dots, X_n) = [LUB(RL(X_1), RL(X_2), RL(X_3), \dots, RL(X_n)), LUB(RH(X_1), RH(X_2), RH(X_3), \dots, RH(X_n)))]$

RL은 클래스나, 속성, 메소드의 하한이고, RH는 상한이다.

클래스는  $Class=(W, X, Y, Z)$ 라고 정의하고, 클래스의 애트리뷰트는  $Attribute=(A, B, C)$ , 메소드는 M이라고 정의한다. 일반적인 상속의 형태를 고려한 보안속성은 다음과 같다.

[속성1] 계층 상속

하위 클래스 Y의 보안등급은 상위 클래스 X의 보안등급을 지배한다.

[속성2] 보안등급 순서 유지

클래스 Y가 클래스 X의 하위 클래스이고  $level(X.A) \geq level(X.B)$ 이면,  $level(Y.A) \geq level(Y.B)$ 이어야만 한다.

[속성3] 제한 상속

클래스 Y가 클래스 X의 하위 클래스이고, Y.A가 X.A에서 상속된 애트리뷰트이면 Y.A의 보안등급은  $level(Y.A)=CGF(X.A, Y)$ 이다.

[속성4] 포함 상속

상위 클래스 X와 하위 클래스 Y는 포함 상속 관계에 있고,  $Y_i.A$ 가 상위 클래스 X에서 상속받는 속성이라 한다면,  $L(Y_i.A)=CGF(X.A, Y_1, Y_2, \dots, Y_n)$ , 단,  $i=1, 2, \dots, n$ 이다.

[속성5] 중복 상속

클래스 Y가 클래스 X의 하위 클래스이고 Y.M이 X.M의 중복된 메소드라고 하면  $level(Y.M)=CGF(X.M, Y)$ 이다

[속성6] 다중 상속

클래스  $X_i$ 가 클래스 Y의 상위 클래스이고 Y.A가  $X_i.A(i=1, 2, \dots, n)$ 에서 다중 상속받는다면,  $level(Y) \geq CGF(X_1, X_2, \dots, X_n)$ 이다. 또한  $level(Y.A) \geq CGF(X_1.A, X_2.A, \dots, X_n.A, Y)$ 이다.

[속성7] 혼합 상속

클래스 Z와 W는 X의 중첩 상속이며 클래스 W는 클래스

X와 Y의 다중 상속 관계가 중첩되어 있다. 이 때 속성 A가 다중 상속받는다면  $level(Z.A)=level(W.A)=CGF(X.A, Y.A, Z, W)$ 이다.

**3. 다중 상속을 위한 보안속성의 확장**

**3.1. 중복 메소드 상속 속성**

지금까지 객체지향 데이터베이스 모델에서 정의되었던 보안속성에 대해서 알아보았다. 앞 절에서 살펴본 모든 보안속성들은 단지 클래스 사이의 보안등급을 어떻게 정의해야하는지를 고려했다. 다중상속에서는 상위 레벨 클래스에 동일한 이름이지만, 서로 다른 작업을 수행하는 메소드가 있다면 어느 것을 상속받을 것인지 고려해야만 하기 때문에, 선택적 상속이 필요하게 된다. 따라서 시스템 구현에 있어서 클래스의 다중상속에 해당하는 규칙으로 정의하면 된다. 중복된 메소드를 선택함에 있어서 속성은 다음과 같다.

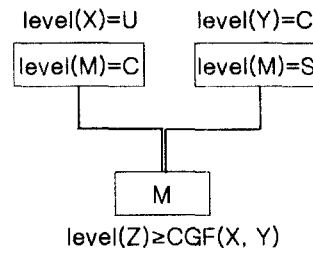


그림 1. 중복 메소드 상속

[속성8] 중복 메소드 상속

클래스 Z로 상속되는 메소드의 보안등급은  $level(Z.M) \geq CGF(X.M, Y.M)$ 이 되고, 상속될 메소드는 아래 선택 함수에 의해서 정해진다.

• 중복 메소드의 선택 함수

```
SelectAttribute(Class X, Class Y)
{
  If (level(X.M) ≥ level(Y.M))
    Z.M = X.M;
  else
    Z.M = Y.M;
}
```

(그림 1)의 경우에는 앞 절에서 정의된 [속성6]에 의해서 클래스의 등급은 정의가 된다. 또한 상속되는 애트리뷰트의 등급도 정의가 되지만, [속성5]와 [속성6]에서는 중복 메소드의 상속이 있을 때 어느 메소드를 상속하는지 정의가 불분명하기 때문에 [속성8]을 필요로 한다. 물론 메소드의 등급은 상속되어질 메소드의 등급을 갖게 된다.

**3.2. 개선된 다중 상속 속성**

기존의 보안 속성들은 새로운 클래스를 정의하는 경우를 고려한 것이었다. 하지만, (그림2)와 같이 일반적인 상속 관계가 있을 때, X가 W와 Z의 하위 클래스로 정의

되어야만 할 경우가 있다. 이런 경우에는 기존의 보안 상속 속성으로는 Y의 보안등급은  $level(Y) \geq CGF(X, W, Z)$ 으로 정의된다. 이런 상속의 경우에는 클래스 Y를 액세스할 수 있었던 사용자에게 대한 권한이 새로운 클래스 계층에서 상실되게 된다. 따라서, 자기 자신의 고유 등급은 계속 가지면서, 보안등급 함수를 이용해서 상속 속성을 정의한다.

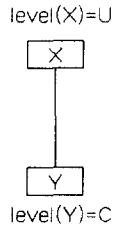


그림 2. 일반적 상속 관계

다중 보안등급 함수의 정의는 다음과 같다.

• 다중 보안등급 함수 (MCF : Multiple Classification Function)

$MCF((X), (Y_1, Y_2, \dots, Y_n)) = [level(X), CGF(Y_1, Y_2, \dots, Y_n)]$ , ( $Y_1, Y_2, \dots, Y_n$ 는 X의 상위 클래스로 정의될 클래스)

단, 보안속성을 위배하지 않기 위해서  $level(X)$ 의 보안등급은 상속계층에서 묵시적으로 상속되지 않는다.

[속성9] 다중 상속 클래스 정의

클래스 X의 하위 클래스인 Y의 보안등급은 새로운 클래스 계층 구조에서 상위 클래스 X뿐만이 아니라, X의 상위 클래스와 자신의 보안등급을 고려한  $level(Y) = MCF(level(Y), RH(X))$ 가 된다.

따라서, (그림3)과 같이 보안등급함수를 적용함으로써 새로운 상속 계층에 대한 정의 없이도 클래스를 사용할 수가 있다.

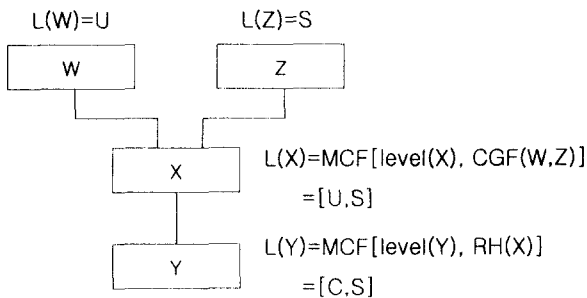


그림 3. 개선된 다중 상속

4. 결론 및 향후 연구방향

관계형 데이터베이스에서 많이 논의되었던 정보 유출 등의 정보 보안 문제가 객체지향 데이터베이스에 적용된

것은 80년대 후반부터 시작되었다.

하지만, 객체지향 데이터베이스에서 사용되는 보안등급과 정책은 새로운 보안 모델이 제시할 때마다 그 개념과 적용범위가 다르게 정의되어왔다.

지금까지 데이터베이스에 대한 객체 지향적 시스템 적용이 꾸준히 연구되어왔지만, 클래스 계층에서 상속에 대한 정의는 개념적인 속성 정의에만 국한되어왔다.

이 논문에서는 객체지향 데이터베이스에서 정의되었던 다중상속의 일반적인 개념과 기존의 객체지향 데이터베이스의 보안모델에서 제시되었던 보안속성들에 대해서 알아보았고, 정의된 보안속성([속성1-7])에서 미흡하게 다루었던 다중상속을 고려한 보안속성([속성8,9])들을 제시하였다.

다중상속에 따른 새로운 보안속성은 중복 메소드 상속에 따른 문제점의 제시와 선택 함수가 정의되었고, 일반적인 상속 관계에서 다중 상속이 추가되었을 때의 클래스의 보안등급을 정해주는 속성을 정의했다. 이러한 다중상속에 따른 보안속성의 제안은 기존에 정의된 상속속성과 함께 객체지향 데이터베이스를 위한 보안 모델을 제시할 때 유용하게 활용될 것이다.

앞에서 제안된 보안속성도 완벽한 객체지향 데이터베이스를 모델링 하기에는 아직까지 부족한 부분이 많이 존재한다. 따라서 향후 상속뿐만 아니라 버전(version), 복합객체(complex object)등에 대한 새로운 보안속성의 연구가 진행되어야 할 것이다.

5. 참고 문헌

[1] James M. Slack, "Security In An Object-Oriented Database", ACM SIGSAC on New Security Paradigms Workshop, pp.155-159, 1993.  
 [2] Zhou Jian, "The Design Analysis of A Multilevel Secure ODBMS", International Conference on Communication Technology, vol.1, pp.5, Oct., 1998.  
 [3] Jay Banerjee, Hong-Tai Chou, Jorge F. Garza, Won Kim, Darrell Woelk, and Nat ballou, "Data Model Issues for Object-Oriented Application", ACM Transactions on Office Information Systems, Vol.5, No.1, Jan., 1987.  
 [4] Jonathan K. Millen, Teresa F. Lunt, "Security for Object-Oriented Database Systems", IEEE Computer Society Symposium, pp.260-272, 1992.  
 [5] Silvana Castano, Mariagrazia Fugini, Giancarlo Martella, and Pierangela Samaratti, "Database Security", Addison Wesley, pp.396-428, 1995.  
 [6] 주광로, 박우근, "데이터베이스 시스템의 보안 기술", 정보처리학회논문지, 제4권, 제2호, pp.33-43, 1997.  
 [7] 노봉남, 김용성, 장옥배, "다단계 객체지향 계층구조에서 상속의 보안 성질", 정보과학회논문지, 제20권, 제9호, 1998.