다단계 보안을 갖는 공간 뷰를 이용한 정보 흐름 제어

전영섭*, 오영환*, 이순조**, 임기욱***, 배해영*
*인하대학교 전자계산공학과
**서원대학교 전자계산학과
***선문대학교 산업공학과
inhaop@hitel.net

Information flow control using spatial view with multilevel security

Young-Sub Jun*, Young-Hwan Oh*, Soon-Jo Lee**, Ki-Wook Rim***, Hae-Young Bae*
*Dept. of Computer Science & Engineering, Inha University
**Dept. of Computer Science, Seowon University
***Dept. of Industrial Engineering, Sunmoon University

요 약

공간 데이터베이스에서는 공간 객체에 대해 객체마다 서로 다른 보안 등급을 설정함으로써 공간 객체에 대한 보안을 유지하고 있다. 다단계 보안을 사용하여 사용자의 보안 등급에 따라 공간 객체에 대한 접근을 제어할 경우 인접 객체와의 위상관계를 통해서 공간 정보 뿐만 아니라 비공간 정보의 노출(information flow)이라는 문제가 발생하게 된다. 이에 대한 해결책으로 데이터베이스에 대한 부분집합만을 추출하여 사용자의 권한에 맞는 질의 결과를 제공하는 것이다. 즉 공간 뷰를 정의함으로써 사용자 등급에 맞는 결과 집합(result set)을 제공함으로써 보다 효율적인 연산을 수행할 수 있게 된다.

따라서 본 논문에서는 실세계의 지리 객체들에 대한 다양한 사용자 관점과 다단계 보안 등급을 가진 뷰를 지원하기 위해 관계형 데이터베이스의 뷰 개념을 확장한 공간 데이터베이스의 공간 뷰를 제안하고, 공간 연산 시 발생하는 정보 흐름 제어를 위한 방법을 제시한다.

1. 서론

공간 데이터베이스 시스템에서의 데이터베이스 보안은 매우 중요한 문제중의 하나이다. 예를 들어, 접근이 불가능한 사용자가 공간 데이터베이스를 가진 군 지리 정보 시스템상의 군사기밀 지역이나, 대도시의 가스 배관망 시스템을 탐지하여 유출하는 행위는 국가나 사회에 엄청난 결과를 초래할 수 있다.

데이터베이스 보안은 권한이 없는 사용자를 제어하여 정보의 불법적인 접근, 고의적인 파괴 및 변경을 방지하고 우발적인 사고로부터 정보를 보호하는 것이다. 즉 데이터베이스 관리 시스템은 데이터베이스에 저장되어 있는 데이터에 대한 불법적인 접근, 고의적인 파괴, 변경, 그리고 비일관성을 발생시키는 접근으로부터 데이터를 보호하기 위하여 보안 정책을 수행하여야 한다[2, 3].

현재까지 데이터베이스 보안을 위한 연구들이 많은 부분에서 이루어지고 있지만 공간 데이터베이스를 위한 보안에 대한 연구는 거의 이루어지고 있지 않다. 공간 데이터베이스 의 경우 공간 데이터와 비공간 데이터를 동시에 다루기 때문에 관계형 데이터 모델에서 다루던 튜플이나 필드 수준에서의 다단계 보안 정책으로는 이를 관리하기가 어렵다.

따라서 본 논문에서는 기밀한 공간 데이터에 대해 서로 다른 등급을 가진 사용자가 접근할 경우, 사용자의 등급에 따른 공간 뷰를 제공함으로써 기밀 데이터에 대한 접근 제어 방법을 제시한다. 또한 질의 결과 집합이 서로 다른 등급의 객체간의 공간 연산일 경우 위상 정보 흐름이라는 문제가 발생하는데 이에 대해 공간적 의미 무결성을 유지하는 방법과 비공간 데이터에 대해 비밀 경로를 통한 정보 흐름 문제 해결을 위한 방법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 다단계 공간 뷰를 위한 관련 연구를 설명하고, 3장에서는 다단계 공간 뷰를 위한 공간 모델을 제시한다. 4장에서는 공간 뷰를 이용한 정보흐름에 대해 기술한다. 마지막으로 5장에서는 결론과 향후 연구에 대해 기술한다.

2. 관련 연구

본 장에서는 관련 연구로서 다단계 보안 모델과 다단계 관계형 데이터베이스 모델에 대해 설명한다.

2.1 다단계 보안 모델

액세스 제어를 위한 보안 정책은 임의적 접근 제어

* 본 연구는 정보통신부의 대학 S/W 연구 센터 지원사업의 연구 결과임

(discretionary access control: DAC) 정책과 강제적 접근 제어(mandatory access control: MAC) 정책으로 구분할 수 있다. DAC 정책은 주체나 주체가 속해 있는 그룹들의 식별자를 근거로 객체에 대한 액세스를 제한하는 방법이며, MAC 정책은 객체에 포함된 정의의 비밀 등급과 주체에 부여된 등급별 비밀 취급 인가를 기반으로 하여 객체에 대한 액세스를 제어하는 방법이다. MAC 접근 모델의 대표적인 예로 다단계 보안 데이터베이스 시스템을 위해 사용되는 가장 널리 사용되는 보안 모델인 BLP(Bell-Lapadula)이 있다[1].이 모델은 단순 보안 속성과 제한 *-속성의 두 가지 성질을 가지고 있는데, 첫 번째 성질은 사용자보다 높은 보안등급을 가진 데이터에 대한 접근을 방지하기 위한 것이다. 두 번째 성질은 높은 보안등급을 가진 객체의 정보를 낮은 보안등급을 가진 객체에 옮김으로써 일어나는 잘못된 정보 흐름(information flow)을 방지하기 위한 것이다. 하지만 Bell-LaPadula모델은 상위레벨에서 하위레벨로의 직접적인 정보 흐름을 방지할 수 있으나, 상위레벨 주체가 하위레벨의 주체에게 간접적으로 정보 전달을 허용할 수 있는 비밀경로를 방지할 수는 없다는 문제점을 가지고 있다.

2.2 다단계 관계형 모델

다단계 데이터를 취급하기 위해, 릴레이션 보안 수준에서 속성값 수준의 보안등급을 포함하도록 해야 한다. 속성, 튜플 수준의 보안등급은 속성값 수준의 보안등급에 의해서 정의될 수 있다. 릴레이션 스키마에서 보안등급 레이블(label)을 속성으로 모델링한다. 이런 방법으로 새로운 데이터를 레이블링하기 위한 분류 규칙이 보안등급 속성에 대한 무결성 제약조건으로 표현한다. 그리고 검색은 보안등급 속성 뿐만 아니라 데이터 속성에 대한 값을 선택할 수 있다. [9]

3. 공간 뷰를 이용한 정보 흐름 제어

본 장에서는 공간 뷰를 정의하고 이를 이용한 정보 흐름 제어를 위한 기법을 제안한다.

3.1 보안을 위한 공간 뷰

지리정보시스템(GIS: Geographic Information System)에서 지리 객체(geographic object)를 모델링 할 때 다양한 사용자 요구 조건들이 있으며, 특히 사용자의 관점에 따른 지리 객체의 서로 다른 공간 표현(spatial representation)을 지원하는 것이 매우 중요하다. 또한 권한등급이 다른 사용자에게 보안등급이 상이한 외부 스키마를 제공할 수 있어야 한다. 즉, 공간 데이터베이스에서는 동일한 지리 객체가 사용자들의 관점과 보안 등급에 따라 상이한 공간 표현을 가질 수 있어야 한다[4, 6].
본 장에서는 실세계의 지리 객체들에 대한 다양한 사용자 관점과 다단계 보안 등급을 가진 뷰를 지원하기 위해 공간 관계 데이터베이스의 뷰 개념을 확장한 공간 뷰를 설명한다.

3.2 뷰의 사용

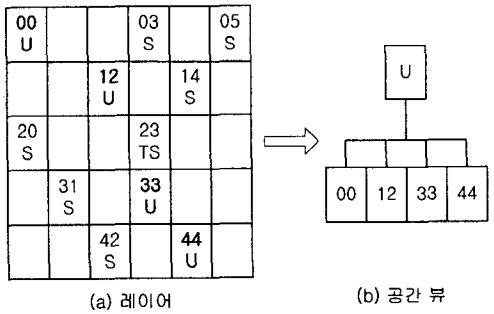
관계 데이터베이스 시스템의 뷰(view)는 저장 데이터(stored data)와 유도 데이터(derived data)를 수학적으로 정의하기 때문에 MLS/RDBMS의 문맥 종속(context-dependant) 및 내용 종속(content-dependant) 보안 분류, 동적 분류(dynamic classification), 추론(inference) 및 집단화(aggregation) 등을 처리하는 수단으로 제안되고 있다[5, 7]. 보안의 목적으로 뷰를 사용하는 개념은 CODASYL과 IBM의 System R로부터 유래된다. System R에서 뷰는 구조적 질의어 SQL로 표현되는 유도 릴레이션이다. System R의 접근 제어 메커니즘은 뷰를 권한 부여의 대상으로 간주한다.
MLS/RDBMS의 기반으로써 뷰의 사용은 Claybrook과 Denning에 의해서 처음 제안되었다. SRI의 SeaView는 다단계보안을 위한 뷰의 사용 개념을 지원하는 최초의 관계 데이터베이스 관리 시스템을 구현한 프로젝트로 MLS/RDBMS 분야의 연구를 상당히 진전시켰다. SeaView에서 제안된 TCB 분할 개념에 의하면 다단계 릴레이션은 단일 단계 기본 릴레이션(single level base relation) 상의 뷰로써 구현된다. 각각의 단일 단계 릴레이션은 다시 참조 모니터(reference monitor)에 의해서 보호되는 하나 이상의 단일 단계 세그먼트(segment) 혹은 화일에 사상 된다[3, 8]. 따라서 각 주체는 자신의 접근 등급이 데이터가 저장되는 객체의 접근 등급을 지배(dominate)하지 않는 한 다단계 릴레이션을 유도하기 위해 기본 릴레이션 내의 어떠한 데이터에도 접근할 수 없기 때문에 데이터베이스 보안을 위한 강제적 접근 제어의 요구사항을 충족시킬 수 있게 된다. 다단계 릴레이션을 뷰로써 구현하는 것은 다단계 릴레이션에 대한 삽입, 삭제 및 갱신 연산이 단일 단계의 저장 릴레이션에 대한 연산으로 전환될 수 있도록 해야 한다.

3.3 다단계 공간 뷰의 유도

본 논문에서 제안하는 다단계 공간 뷰(MLSView/SRDM)는 공간 데이터를 위한 객체 개념을 기본으로 지원하고 뷰를 수행하여 그 결과를 물리적으로 데이터베이스에 저장하는 실체화 방법을 이용한다. 그 이유는 소스객체의 식별자만을 저장하는 객체 지향 뷰 실체화 방법을 이용하면 질의 수행 속도가 오래 걸리기 때문이다. 이는 기하데이터가 변형된 공간 뷰인 경우에는 질의를 수행하기 위하여 매번 소스 객체들에 대하여 공간 연산을 수행하기 때문이다. 이를 해결하기 위하여 본 논문에서는 실체화된 공간 뷰 객체에 데이터를 복사하여 저장하는 방법을 이용한다. 본 연구에서 제안하는 공간 뷰는 다음과 같은 특징을 가진다.
(1) 저장된 공간 객체를 공간 데이터와 비공간 데이터의 속성값 단위로 사용자가 부분적으로 접근 또는 추출할 수 있어야 한다. 이와 관련된 모든 데이터는 실제 데이터로 실체화하여 저장한다.
(2)유도된 데이터에 대한 공간 연산이 별도로 필요하다. 따라서 저장데이터를 갖는 클래스에 허용된 연산 중 필요한

일부를 선택할 수 있어야 하며, 또한 유도 데이터에만 적용할 수 있는 새로운 연산을 정의할 수 있어야 한다.
(3)기본 공간객체에 접근을 허가 받지 못한 사용자는 접근 허가 권한이 낮은 공간 뷰를 통해 공간 데이터에 접근할 수 있다. 이는 사용자 관점에 따른 다양한 공간 표현과 보안 등급을 제공한다.
(4) SRDM에서 제공하는 통합 뷰, 공간 레이어, 타일 단위의 보안 등급이 동일한 공간 뷰를 생성하여 사용자의 보안 등급 단위로 관리하도록 한다.
(5) 공간 뷰를 통한 데이터 접근시 사용자는 데이터가 실제로 어디에 저장되어 있는 지는 인식하지 못하고, 공간 뷰를 접근하도록 한다. 이를 통해서 논리적 데이터의 독립성을 높인다.

다음 [그림 1]은 레이어가 여러 개의 다단계 타일로 분할 관리되고 있을 때 사용자의 접근 등급에 맞는 공간 뷰를 생성하는 예를 보인 논리적 개념도이다. 한 사용자의 접근 등급이 U 일 때 한 레이어에서 U 등급인 타일만을 선택하여 이를 별도의 저장 뷰로 관리한다.



(a) 레이어 (b) 공간 뷰

[그림 1] 다단계 공간 뷰의 유도

3.4 다단계 공간 뷰의 정의

다단계 공간 뷰(MLSView/SRDM)는 객체 지향 뷰의 정의와 마찬가지로 공간 뷰를 위한 정의 구문은 뷰-정의 질의(view-definition query)와 스키마 요소(schema elements)로 구성된다. 공간 뷰가 정의되면 MLS/SRDM에서의 메타 데이터처럼 공간 뷰 메타 데이터가 생성된다.
공간 뷰를 정의하기 위한 구문은 다음과 같다.

```
MLSview  SViewName(Attributes, Geom, sLevel)
AS       SELECT          Attributes, Geom
         FROM            SourceClass
         [ WHERE         Predicates ]
         [ New_Attributes  new-attributes ]
         [ New_Methods     new-methods ]
```

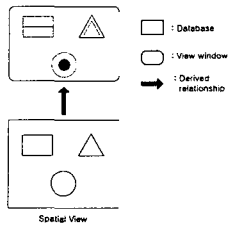
[그림 2] 공간 뷰 정의문

본 논문에서는 공간 뷰-정의를 위하여 특정한 질의어가 아닌 일반적인 객체 지향 질의어를 사용하는 것을 전제로 한다. 스키마 요소에서 어트리뷰트 정의는 비공간 어트리뷰트와 기하 데이터를 표현하기 위하여 Geom 어트리뷰트를 정의한다. *sLevel* 은 공간 뷰의 접근 등급 레벨을 부여한다.
공간 뷰-정의 구성은 다음과 같다. SELECT 절에 있는 공간 뷰의 어트리뷰트들의 값들은 소스클래스의 어트리뷰트들과 새로운 어트리뷰트로부터 유도되며, 새롭게 정의된 속성은 소스 클래스에 없는 새로운 속성을 뷰 클래스에 정의한 것으로 이는 뷰 클래스의 메소드에 의해서 정의되어 진다. Geom 어트리뷰트의 값은 뷰-정의 질의에서 기술된 공간 함수에 의해 유도된다. FROM 절은 공간 뷰 추출에 기본이 되는 소스 클래스들을 명시하며, 여러 개의 기본 클래스나 뷰 클래스로부터 뷰를 생성할 수 있다. WHERE 절은 생략될 수 있으며, 공간 뷰를 통하여 유도되는 데이터에 대한 것으로서, 기존의 SQL 프레디키트나 불린(boolean) 값을 가지는 연산자들이 될 수 있다. 또한 공간 함수를 포함한다. New_Attributes 절은 소스 클래스에 없는 새로운 속성을 정의하기 위한 것으로 이는 메소드에 의해 정의된다. New_Methods 절은 소스 클래스에 없는 새로운 메소드를 정의한 것으로 실체화된 공간 뷰만을 위해 생성된다.
다음은 다단계 구조의 하나인 동일한 보안 등급을 가진 타일기반의 공간 뷰의 생성 과정을 보여준다. 접근 등급이 U인 사용자를 위해서 빌딩 레이어의 접근 등급이 U 인 타일만을 선택하여 하나의 공간 뷰를 생성한다.

```
MLSView      Unclassified_Building(*, NULL, U)
AS  SELECT   *
      FROM   Building.Layer
      WHERE  TileDic.SecurityLevel = U;
```

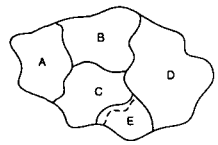
3.5 정보 흐름 제어

정보 흐름이라는 것은 다단계 보안 모델에서 보안 등급이 높은 객체에서 보안등급이 낮은 객체로의 정보 노출을 말한다. 공간 데이터베이스의 경우 관계형 데이터베이스에서의 정보 흐름 뿐만 아니라 공간 객체들 사이의 위상 연산을 통해 발생할 수 있는 위상 정보 흐름을 제어해야 한다. 본 논문에서는 위에서 정의된 공간 뷰를 통한 제어를 살펴보자.
공간 뷰는 유도되는 기하 데이터에 따라 기하 변환을 동일한 공간 차원의 변환과 상이한 공간 차원의 변환으로 나눌 수 있다. 동일한 공간 차원의 변환은 공간 뷰의 기하 데이터 도메인이 소스 클래스와 같다. 예를 들어 점에서 점으로의 변환(point-to-point transformation)이 이 경우에 속한다. 반면에 상이한 공간 차원의 변환은 공간 뷰의 기하 데이터 도메인이 소스 클래스와 다른 경우로, 점에서 면으로의 변환(point to area transformation)하는 경우가 여기에 속한다.



[그림 3] 뷰 윈도우

위와 같은 방법으로 유도된 공간 뷰(derived spatial view)가 [그림 3]과 같이 기하 데이터에 대한 변형을 제공함으로써 출력되어진 결과를 통해 보안을 유지할 수도 있지만, 이럴 경우 위상 관계에 의한 의미적 무결성을 위배라는 문제가 발생하게 된다.



[그림 4] 구경계 레이어

의미적 무결성 위배의 예로는 [그림 4]와 같은 구 경계 레이어가 있을 경우, 기밀한 데이터를 가진 구가 존재하여 이 구 객체의 보안레벨을 높게 주고, 공간 뷰를 생성시 이 지역을 버퍼링 시켜 확장하거나 좌표 값을 수정하게 되면 위상관계에서 항상 상접(meet)되어 있어야 할 구 경계가 겹치게(overlap)되는 경우를 들 수 있다.

이와 같은 경우 기하 데이터의 변형 없이 위상 관계에 의한 위상 정보 흐름을 제어하기 위해서는 위상 정보 흐름 모델(Topological Information Flow Model)에 따라 보안 등급이 높은 객체의 보안 등급을 낮은 객체의 보안등급으로 낮춤으로써 해결할 수 있다. 그런데 다단계 공간 데이터베이스 모델에서는 공간 객체 자체 뿐만 아니라 객체에 대한 속성 정보까지 포함하고 있기 때문에 보안 등급을 낮추게 될 경우 객체 자체의 보안 등급을 낮추면서 보안 등급이 높은 필드에 대해서는 속성 값을 NULL로 대체함으로써 공간 뷰를 통한 다단계 보안을 적용할 수 있다. 따라서 공간 뷰를 제공함으로써 공간 뷰도 공간 객체와 마찬가지로 다단계 보안을 지원할 수 있다.

4. 결론 및 향후 연구

기밀이 요구되어지는 공간 데이터베이스의 경우, 출력되어진 객체들의 위치 정보나 인접한 객체와의 위상 관계를 통해서 많은 정보가 노출되어질 위험이 있으므로 엄격한 사용자의 접근제어가 요구되어진다. 다단계 보안 등급을 적용할 경우 다른 공간 객체들 사이의 위상관계를 통해서 상위 보안등급 객체에 대한 정보의 대략적인 유추가 가능하다.

보안을 위해 공간 객체의 질의결과를 변형할 경우 의미적 무결성 위배라는 문제가 발생하게 되고, 비공간 정보에 대해서는 기밀데이터에 대한 유추가 가능하게 된다. 따라서 공간 객체에 대해 공간 연산과 비공간 연산의 결과에 있어 의미적 무결성을 유지하면서 정보 흐름 제어를 위한 공간 뷰를 제공함으로써 다단계 보안을 유지할 수 있게 된다.

향후 연구과제로는 데이터베이스의 접근을 위해 공간 뷰를 구성할 경우 효율적인 접근 제어를 위해 레이어 상의 객체에 대한 보안 등급의 적용 단위(granularity)로 타일을 사용할 경우와 하나의 타일에 포함될 서로 다른 등급을 갖는 보안 객체의 수를 어떻게 결정하고 객체가 여러 레이어에 걸쳐 있을 경우 효율적인 타일 분할을 어떻게 할 것인가 하는 것이다.

5. 참고문헌

[1] T. Y. Lin, "Bell and Lapadula Axioms: A "New" Paradigm for an "Old" Model," *Proc. of 1992-1993 ACM SIGAC New Security Paradigms Workshop,* pp.232-243, Dec. 1993.

[2] O. Costich, M. H. Kang and J. N. Froscher, "The SINTRA Data Model : Structure and Operations," *Proceedings of the IFIP WG 11.3 Workshop on Database Security*, pp. 97 - 110, Aug. 1994.

[3] T. F. Lunt and E. B. Fernandez, "Database Security," *SIGMOD Record*, Vol. 19, No. 4, pp. 90 - 97, Dec. 1990.

[4] Claramunt C. and Mainguenaud M., "Identification of Definition Formalism for a Spatial View," *Advanced Geographical Modeling*, 1994.

[5] S. G. Akl and D. E. Denning, "Views for Multilevel Database Security," *Advances in Computer System Security*, VOL.III, Artech House Inc., pp.223-233, 1988.

[6] R. Laurini and D. Thompson, 'Fundamentals of Spatial Information Systems,' Academic Press, 1992.

[7] J. Wilson, "Views as the Security Objects in a Multilevel Database Management Systems," *Proc. of 1988 IEEE Symposium on Security and Privacy*, pp.70-84, Apr. 1988.

[8] T. F. Lunt, D. E. Denning, R. R. Schell, M. Heckman and W. Shockley, "The SeaView Security Model," *Proc. of 1988 IEEE Computer Society Symposium on Security and Privacy*, pp.218-233, 1988.

[9] 심갑식, 노봉남, "다단계 보안 데이터 모델", 통신정보보호 학회지, 제2권 제3호, 1992