공간 데이터베이스의 보안을 위한 타일 단위의 접근 제어 기법

°강 동 재*, 오 영 환*, 김 재 홍**, 배 해 영*
*인하대학교 전자계산공학과
**영동대학교 컴퓨터공학과
baramsori72@cjdream.net

A Tile-based Access Control Method for the Security of Spatial Database

°Dong-Jae Kang*, Young-Hwan Oh*, Jae-Hong Kim**, Hae-Young Bae*
*Dept. of Computer Science & Engineering Inha University
**Dept. of Computer Engineering Youngdong University

요 약

공간 데이터베이스를 권한이 없는 사용자의 접근, 고의적인 파괴 혹은 우발적인 사고로부터 보호하기 위하여 공간 데이터베이스에 대한 보안정책의 수용이 필요하다. 보안등급의 적용 단위는 필드, 객체, 레이어 단위의 방법이 있으며, 객체 단위의 보안등급 적용은 인접한 객체의 위상관계에 의한 정보 유출의 문제점이 있고, 레이어 단위 보안등급의 적용은 공간 객체에 대한 사용자의 접근성을 저하시키는 문제를 발생시킨다.

본 논문에서는 공간 객체에 대한 사용자의 접근성을 향상시키기 위하여 타일 단위의 접근제어 기법을 제안한다. 타일 단위 접근제어 기법은 보안등급 적용 단위를 타일(Tile)로 하며 레이어, 지도의 보안등급은 하위 수준인 타일과 레이어에 부여된 보안등급의 최하위 등급으로 각각 설정한다. 제안한 기법의 구현을 위해 타일의 구조와 스키마를 정의하고, 보안 유지를 위한 연산 제약사항을 기술한다. 연산 제약 사항은 기본적으로 BLP의 속성을 따르고, 상위 등급 객체에 대한 수정 방지와 하위 등급 객체에 대한 수정 허용을 위해서 BLP 속성을 확장한다.

제안된 기법은 레이어 단위의 접근제어 기법에서 발생하는 문제점을 해결하여 객체에 대한 사용자의 접근성을 향상시키며 인접한 객체 사이의 위상관계에 의한 정보의 유출을 방지한다.

1. 서 론

공간 데이터베이스의 보안은 공간 데이터베이스내의 데이터에 대한 권한이 없는 접근, 고의적인 파괴 혹은 변경 그리고 비일관성을 발생시키는 우발적인 사고로부터 데이터 또는 공간 데이터베이스를 보호하는 것을 의미한다[5].

현재까지 데이터베이스의 보안을 위한 연구들이 많은 부분에서 이루어지고 있지만 공간 데이터베이스를 위한 보안에 대한 연구는 거의 이루어지고 있지 않다. 공간 데이터베이스의 경우 대부분의 어플케이션들이 그래픽 유저 인터페이스를 사용하고 있기 때문에 기밀이 요구되어지는 공간 데이타베이스의 경우, 출력되어진 객체들의 위치 정보나 인접한 객체와의 위상관계를 통해서 많은 정보가 노출되어질 위험이 있으므로 엄격한 사용자의 접근제어가 요구되어진다. 이러한 접근제어의 단위로 레이어 단위의 접근제어를 공간 데이타베이스에 적용하는 경우, 객체와 레이어에 대한 사용자의 접근성이 저하되며 객체 단위의 접근제어를 적용하는 경우는 인접 객체들 사이의 위상관계에 의한 기밀한 공간 데이터의 정보 유출이라는 문제가 발생한다.

본 논문에서는 이러한 공간 데이터베이스의 특성을 고려하여 타일 단위의 접근제어 기법을 제안한다. 타일 단위 접근제어 기법은 보안등급 적용 단위를 타일(Tile)로 하며 레이어, 지도 수준의 보안등급은 하위 수준인 타일과 레이어에 부여된 보안등급의 최하위 등급으로 각각 설정한다. 제안한 기법의 구현을 위해 타일의 구조와 스키마를 정의하고, 보안 유지를 위한 연산 제약사항을 기술한다.

공간 데이터베이스에 타일 단위 접근제어 기법의 적용은 객체 단위의 접근제어에서 발생하는 인접한 객체들 사이의 위상관계에 의한 정보의 노출을 줄일 수 있고 레이어 단위의 접근제어에서 발생하는 객체와 레이어에 대한 사용자의 접근성 저하라는 문제를 개선한다.

본 연구는 정보통신부의 대학 S/W 연구센터 지원사업의 연구 결과임

2장에서는 보안등급의 적용 단위(granularity)와 기존의 레이어 단위의 접근제어에 대한 관련 연구를 살펴본다, 3장에서는 타일 단위 접근제어 기법의 전략과 타일, 레이어, 지도에 대한 보안 등급, 타일단위 접근제어를 지원하기 위한 구조 및 스키마에 대해서 정의하고 타일 단위의 접근제어에서 보안을 유지하기 위한 연산 제약사항을 기술한다. 마지막으로 4장에서는 제안된 기법에 대한 상점과 향후 연구 내용을 정리한다.

2. 관련 연구

2.1 보안 등급의 적용 단위(granularity)와 정책

공간 데이터베이스의 보안을 위한 접근제어를 구현하기 위해서는 보안등급을 적용하는 단위와 보안의 정책을 결정해야 한다.

일반적인 경우, 다단계 데이터베이스 시스템은 보안등급을 적용하기 위한 단위로서, 원자적 사실, 즉 튜플(tuple)의 필드(field)마다 각각 보안등급을 부여하며 그로부터 튜플과 테이블에 대한 보안등급을 결정하게 된다[6].

공간 데이터베이스의 보안을 적용하기 위한 단위로 필드 단위의 보안등급을 부여한다는 것은 일반적으로 대용량의 데이터로 구성되는 공간 데이터베이스 시스템에 커다란 부하가 된다. 또한 공간 데이터베이스에서는 인접한 객체들 사이의 위상관계를 통해서 정보가 누출되어질 수도 있으므로 밀접한 위상관계를 가지는 주변의 객체들도 함께 보안의 대상이 되는 것이 바람직하다 .

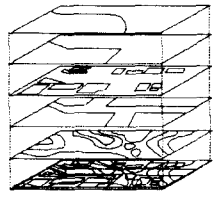
보안을 유지하기 위한 보안 정책으로는 데이터에 대한 사용자의 권한을 제어하는 접근 제어 방식 (Access Control)을 가장 많이 사용하며 이러한 접근 제어를 위한 보안정책은 임의적 접근 제어 (Discretionary Access Control, DAC)와 강제적 접근제어(Mandatory Access Control ,MAC)로구분된다[1]. 강제적 접근제어의 경우 BLP(Bel-lLaPadula)의 속성인 단순속성(simple property)과 *-속성(star-property)을 따른다[6]. 단

순속성은 주체(사용자)의 인가등급이 객체의 분류등급보다 같거나 높은 경우에만 주체는 객체를 판독(read)하는 것이 허용된다는 것을 규정하며 *-성질은 주체의 인가등급이 객체의 분류 등급보다 같거나 낮은 경우만 주체는 객체에 대한 기록(write)이 허용되어지는 성질을 말한다.

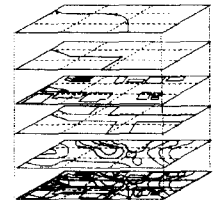
공간 데이터베이스에서 *-속성을 그대로 적용하면 상위의 인가등급을 가진 사용자가 하위의 분류등급을 가지는 객체에 대한 쓰기(write)연산을 할 수 없게 되는 문제가 발생된다.

2.2 공간 데이터베이스의 레이어 단위의 접근제어

공간 데이터베이스 시스템에서 관리하는 지리 데이터는 각각의 주제별로 그 주제에 속하는 공간 객체들의 집합을 하나의 레이어로 관리한다. [그림1]은 레이어로 분할하여 지리 데이터를 관리하며 이들 레이어를 조합하여 지리 데이터를 구성하는 것을 보인 것이다[2].



[그림1] 레이어를 이용한 지리 데이터의 분할 및 통합



[그림2] 타일로 분할된 지리데이터의 레이어

지리 데이터를 레이어 단위로 분할하여 관리하는 방식은 기존의 지리정보 시스템에서 많이 사용되는 지리 데이터 관리 방식이며[2] 인가 받지 못한 사용자의 불법 검색이나 갱신 등의 보안을 위한 보안등급의 적용 단위로 사용된다.

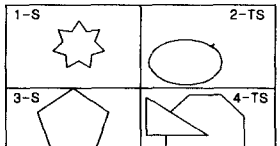
그러나 이러한 방식은 레이어 전체를 지리 정보 시스템의 보안 단위로 사용하기 때문에 한 레이어 위에 존재하는 몇몇의 기밀한 데이터를 보호하기 위해서 그 레이어에 속하는 나머지 객체들에 대한 사용자 접근성을 감소시킨다는 문제점을 갖는다. 이러한 객체나 레이어에 대한 하위 보안등급 사용자의 접근성 향상을 위해서는 보안을 위한 적용 단위의 축소가 요구된다. 레이어는 타일이라는 작은 영역들로 구분할 수 있으며 [그림2]는 레이어를 타일 단위로 나누어 관리하는 것을 보여준다.

3. 타일(Tile) 단위의 접근 제어 기법

공간 데이터베이스에 보안을 적용할 때 발생하는 기존 연구가 가지고 있는 문제점들을 해결하기 위한 방법으로 타일 단위의 접근제어 기법을 제안한다. 본 장에서는 제안하는 기법에 대한 전략과 지도, 레이어, 타일에 대한 보안등급의 정의를 기술하며 구현을 위한 구조 및 스키마를 정의한다. 마지막으로 타일 수준의 접근제어 기법에서 보안을 유지하기 위한 연산 제약사항을 고려한다.

3.1 타일 단위 접근제어 기법의 전략

3.1.1 객체, 레이어에 대한 사용자 접근성의 향상

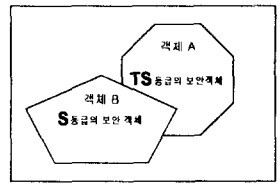


[그림3] 객체에 대한 접근성

그림[그림3]은 서로 다른 보안등급을 가지는 레이어상의 타일들을 나타낸다. 타일에 표시된 분류등급은 타일상의 객체가 가지는 기밀도를 의미한다. [그림3]의 객체들이 레이어 단위의 보안등급으로 관리되어지는 경우, 레이어상의 객체들은 모두 같은 보안등급의 객체로서 인식되어지며 해당 레이어에 요구되는 기밀도를 반영한다. 따라서 [그림3]에서는 모든 객체가 TS 분류등급으로 취급되며 해당 레이어에 부여된 보안등급이 객체들의 보안등급이 된다. [그림3]에서 접근할 수 있는 사용자는 인가등급TS를 가진 사용자만이 허가되며 S등급의 사용자는 객체들에 대한 접근이 거부된다. 이와 같이 레이어 단위의 접근제어 기법은 객체에 대한 사용자의 접근성을 저하시키는 문제점을 발생시킨다.

[그림3]의 객체들에 대해서 타일단위의 접근제어 기법을 적용하는 경우 타일2와 타일4는 TS 보안등급의 객체를 포함하므로 TS의 보안등급을 가지게 되고 해당 객체들은 TS 등급의 객체들로 인식된다. 타일1과 타일3의 경우는 S보안등급만이 존재하므로 S등급이 부여된다. S등급의 사용자가 [그림3]의 레이어에 접근하는 경우 타일1, 타일3에 대해서는 접근이 허용되어지며 타일2, 타일4는 접근이 거부되기 때문에 보안은 유지가 되며 사용자의 접근성을 향상 시킬수 있다.

3.1.2 위상관계에 의한 정보 유출의 방지



[그림4] 인접한 객체의 위상 관계에 의한 정보의 노출

공간 데이터베이스에서 필드 수준이나 튜플 수준의 보안을 지원하는 경우 위상관계에 의한 정보의 노출이 문제가 된다. 공간 데이터의 경우 비공간 데이터와는 달리 위치 정보를 가지고 있으며 주변의 인접한 객체들과의 위상관계가 중요한 요소로서 작용한다. 이러한 인접 객체와의 위상관계를 통해서 상위 보안등급 객체에 대한 정보의 대략적인 유추가 가능하다. 예를 들어 [그림4]에서 S등급의 사용자가 객체 A(TS분류등급)는 객체 B(S분류등급)의 북서쪽에 어느 지점에 위치한다라는 정보를 아는 경우, 또는 객체 A가 객체 B와 인접한다는 정보를 아는 경우, TS 등급의 객체를 볼 수 없지만 객체 B의 위치로부터 객체 A의 대략적인 위치의 유추가 가능하다. 그러므로 공간 데이터베이스에서는 보안이 요구되어지는 해당 객체뿐만 아니라 인접한 객체들에도 보안의 필요성이 요구되어 진다. 따라서 인접한 객체들을 함께 동일한 등급의 보안 객체로 묶을 수 있는 타일이라는 단위로 보안등급을 부여한다. 타일 단위의 보안의 경우 [그림4]의 두 개의 객체를 하나의 보안등급으로 묶어줌으로서 위상관계에 의한 정보의 유출을 감소시킨다.

3.2 타일, 레이어, 지도의 보안등급 부여 정책

다단계의 데이터를 다루기 위해, 레이어 수준의 보안은 타일 수준의 보안등급을 포함하도록 해야 한다. 레이어의 보안등급은 레이어를 구성하는 타일들의 보안등급에 의해서 정의되며 레이어 스키마는 각각의 타일 정보 Ti에 대해서 보안 등급 Ci를 추가함으로서 확장되어진다. Ci의 도메인(domain)은 [Li,Hi]로 정의되고 이것은 가장 낮은 보안등급 Li에서 가장 높은 보안등급 Hi범위의 부분 격자(sublattice)를 나타낸다.

레이어(LR)는 각각의 타일(Tile) Ti에 대해서 보안등급 Ci 가 존재하는 레이어로 정의된다.

LR(T1, C1, T1, C2, ... , Tn, Cn)

이 레이어 LR의 보안등급은 C1, C2, ... ,Cn 의 최대하계(greatest lower bound) 이하의 보안등급이 할당된다. 이러한 부결성 제약조건에 따라서 사용자는 먼저 레이어의 접근 권한을 가진 후에 그 레이어에 속해 있는 타일중의 하나를 접근할 수 있게 된다.

지도(M)의 보안등급은 지도를 구성하는 레이어 LRi에 대해서 보안등급 Ci가 존재하는 지도로서 정의 되어진다.

M(LR1, C1, LR2, C2, ... , LRn, Cn)

지도 M의 보안등급은 LRi의 보안등급인 C1...Cn의 최대하계 이하의 보안등급이 할당된다.

지도의 경우 지리 데이터를 접근하기 위해서 가장 먼저 읽기를 해야 하는 대상이 된다. 따라서 지도는 가장 낮은 보안등급을 부여 받도록 하며 대부분의 사용자의 접근을 허용하는 것이 일반적이다.

3.3 타일 단위 접근제어 기법을 위한 구조와 스키마

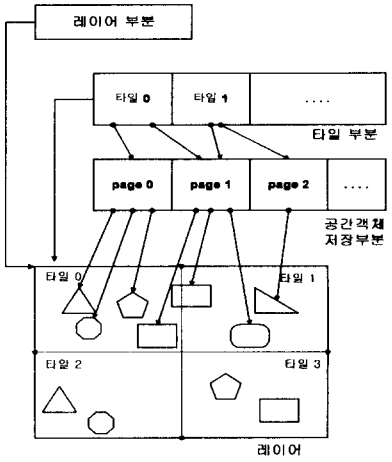
타일 단위의 접근제어를 위해서 레이어를 레이어 부분, 타일 부분, 공간객체의 저장 부분으로 나누어 관리한다. 레이어 부분은 레이어의 전체적인 정보를 저장하며 타일 부분은 타일에 대한 정보와 타일에 속한 공간객체에 대한 정보를 관리한다. 공간객체 저장 부분은 실제의 공간객체를 저장하고 있는 부분으로 페이지들의 집합으로 구성된다. 타일을 관리하기 위해서는 [그림5]과 같은 구조가 필요하며 각각의 레이어와 해당

2)**TS**: TopSecrete **S**: Secrete **C**: Confidential **U**: Unclassified

레이어내에 포함된 타일들을 관리하는 부분에는 보안등급을 위한 부분이 정의되어져야 한다.

[그림6]은 타일 단위의 보안을 지원하기 위해서 [그림5]부분의 레이어 부분과 타일 부분에 보안등급의 관리를 위한 속성을 추가하여 스키마를 확장한 것이다.

지도에 관한 정보를 관리하는 부분에서도 [그림6]과 같이 보안등급의 부여를 위한 부분을 정의한다.



[그림5] 타일 분할된 레이어를 관리하기 위한 구조

```
struct LayerHeader{
  string        name; // 레이어의 이름
  SECURITY      SecurityLevel; // 레이어의 보안등급
  Coordinate    origine;          // 레이어의 원점 좌표
  MBR           totalArea         // 레이어 전체영역의 좌표값
  MBR           tileArea          // 타일 영역의 크기 지정
  int           PageCnt           // 페이지의 개수
  int           PageSize          // 페이지의 크기
  int           PageHeaderOffset//공간객체 저장부의 시작위치
  int           timeStamp          // 레이어의 최종 변경시간
};
struct TileHeader{
  int           tileID; // 타일의 식별자
  SECURITY      SecurityLevel; // 타일의 보안등급
  int           tileLinkOffset   // 타일의페이지링크영역
                                 의 시작 위치
  Int           tileOffset; //  각각의 tile에 대한 링크
  int           timeStamp // 타일의 최근 갱신 시간
}
```

[그림6] 타일수준 보안을 지원하기 위한 스키마

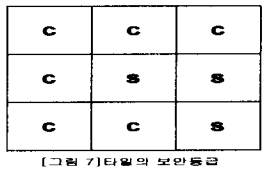
3.4 타일 단위 접근 제어에서의 연산시 제약조건

3.4.1 읽기(read) 연산

읽기 연산의 경우 Bell-LaPadula의 단순속성(simple security property)에 따라서 접근하려는 사용자(주체)의 인가등급이 객체의 분류등급과 같거나 높은 경우에 허용된다. 즉 [그림7]에서 레이어에는 분류등급 C가 부여되며 C인가등급의 사용자는 레이어의 접근 권한을 가지고 분류등급 S인 타일을 제외한 나머지 타일에 대한 접근 권한을 가진다. S인가등급 이상의 사용자는 모든 타일에 대해서 접근 권한이 주어지며 U인가등급 사용자는 레이어 자체에 대한 접근이 거부된다.

3.4.2 객체의 생성 연산

[그림7]와 같이 보안 등급이 부여된 타일에 대하여 객체를 삽입하는



[그림 7]타일의 보안등급

연산의 경우 사용자는 해당 레이어를 접근할 수 있는 보안등급을 가져야 하므로 반드시 C등급 이상의 보안등급을 가진다. 사용자의 보안등급이 C인 경우 레이어 상의 보안등급 S를 가지는 타일의 객체들은 주체로부터 숨겨지게 된다. 사용자는 BLP의 보안 속성에 따라서 접근하려는 타일의 분류등급이 사용자의 보안등급보다 같거나 높은 경우에 대해서 객체의 생성이 가능하다. 낮은 등급의 타일에 대한 쓰기를 허용하는 경우 상위등급의 정보들이 C 또는 U 와 같은 하위등급을 가진 사용자들에게 흘러가는 보안상의 문제가 발생할 수 있다. 하지만 이것은 사용자가 낮은 분류등급의 타일에 대해서 객체의 생성 연산을 할 수 없다는 문제를 발생시킨다.

제안한 기법에서는 접근하려는 사용자가 인증 단계에서 객체를 생성하려는 타일의 보안등급에 맞도록 자신의 보안등급보다 낮은 등급으로 시스템 접근을 허용하므로서 하위 등급의 타일에 대한 객체의 생성 연산을 허용한다. 자신의 보안등급보다 낮은 등급으로 접근 한 사용자는 이전 등급의 타일에 대한 접근이 불가능하므로 정보가 상위의 보안등급에서 하위의 보안등급으로 유출되는 것을 방지된다.

3.4.3 삭제(Delete) 연산과 수정(Modify) 연산

삭제와 수정연산은 접근하는 사용자의 보안등급과 동등한 보안등급을 가진 타일상의 객체에 대해서만 허용한다. 이는 기밀이 요구되어지는 상위 보안등급의 객체를 하위 보안등급을 가진 사용자가 파괴하는 행위를 방지하기 위한 것이다. 하위 보안등급의 객체에 대한 삭제 및 수정은 객체의 생성 연산에서와 같이 시스템 접근시 해당 타일의 보안등급과 동일한 등급의 사용자로서 접근을 허용하므로서 지원한다.

4. 결 론

본 논문에서는 타일단위로 보안등급을 적용하는 타일 단위 접근제어 기법을 제안했다. 타일 단위의 접근제어는 레이어를 구성하는 타일 단위로 보안등급을 적용하고 레이어의 보안등급은 타일의 보안등급에 의해서 결정된다. 제안된 기법의 구현을 위해서 필요한 구조와 스키마를 정의했으며 보안을 유지하기 위한 연산 제약사항을 기술했다. 이러한 타일 단위 접근제어 기법을 공간 데이터베이스에 적용함으로서 레이어와 객체에 대한 사용자의 접근성을 향상시켰으며 인접한 객체들 사이의 위상관계에 의한 기밀한 정보의 유출을 방지할 수 있었다.

향후 연구로는 공간 데이터베이스에 타일 단위의 접근제어 기법을 적용할 때 효과적인 보안을 유지하기 위한 타일의 크기에 대한 사항이 고려되어져야 한다 .

참고 논문

[1] Ravi S. Sandhu, Pierangela Samarati, "Access Control : Principle and Practice"

[2] Cho, Yeong-Seob , "A Client-Side Web GIS Using Tiling Storage Structure and Hybrid Spatial Query Processing Strategy", pp34-57, 1999

[3] Ravi Sandhu, Pieranger Samarati, "Authentication, Access Control, and Audit", CRC Press, 1996

[4] Gabsig Sim, "The Design and Implementation Methodolgy of Multilevel Secure Data Model Using Object Modeling Technique", 통신정보보호학회 논문지, 제8권, 제3호, 1998

[5] 조완수, "Design of an Extended Relational Database System for Multilevel Security", pp42-59, 1996

[6] 심갑식, 노봉남, "다단계 보안 데이터 모델", 통신정보보호학회지, 제2권 제3호, 1992

[7] Ravi S. Sandhu and Sushil Jajodia, "Data and Database Security and Controls", Handbook of Information Security Management, pp481-499, 1993