通信情報保護學會論文誌
第 11 券 第 1 號, 2001. 2

다단계 보안 공간 데이터베이스를 위한 공간 다중인스턴스화

오 영 환**, 이 재 동***, 임 기 욱****, 배 해 영**

Polyinstantiation for spatial data for multilevel secure spatial database

Young-Hwan Oh**, Jae-Dong Lee***, Kee-Wook Rim****, Hae-Young Bae**

요 약

본 논문에서는 다단계 공간 데이터베이스 시스템에서 비밀 위상 경로(covert topology channel)를 해결할 목적으로 공간 다중인스턴스화(polyinstantiation for spatial data)에 대해 연구한다. 위상 구조를 갖는 공간 데이터베이스 시스템은 공간 데이터와 서로 인접한 공간 데이터를 이용하여 다양한 공간 분석을 수행하여야 한다. 그러나, 공간 데이터베이스에서 공간 데이터간의 위상 정보를 지원하는 경우 위상관계에 의한 정보의 노출(information flow)이 문제가 된다. 즉, 공간 데이터베이스를 갖는 지리정보시스템의 경우 대부분의 응용업무가 그래픽 사용자 인터페이스를 사용하고 있기 때문에 기밀이 요구되어지는 공간 데이터베이스의 경우, 출력되어진 객체들의 위치 정보나 인접한 객체와의 위상관계를 통해서 많은 정보가 노출되어질 위험이 있으므로 엄격한 사용자의 접근제어가 요구되어진다. 본 논문에서는 이러한 문제점을 해결하기 위해 MLS/SRDM(Multi Level Security/Spatial Relational Data Model)를 설계하고 공간 데이터의 위상관계로 인해 생기는 정보 유출을 방지하기 위해 공간 다중인스턴스화를 제안한다.

ABSTRACT

In this paper we study the use of polyinstantiation for spatial data, for the purpose of solving covert topology channel in multilevel secure spatial database systems. Spatial database system with topological structure has a number of spatial analysis function using spatial data and neighbored one's each other. But, it has problems that information flow is occurred by topological relationship in spatial database systems. Geographic Information System(GIS) must be needed mandatory access control because there are many information flow through positioning information and topological relationship between spatial objects. Moreover, most GIS applications also use graphic user interface(GUI). In addressing these problems, we design the MLS/SRDM(Multi Level Security/Spatial Relational Data Model) and propose polyinstantiation for spatial data for solving information flow that occurred by topological relationship of spatial data.

keyword : *Multilevel secure spatial database, Information flow, Polyinstantiation*

Ⅰ. 서 론

데이터베이스 보안(database security)의 목적은 권한이 없는 사용자를 제어하여 정보의 불법적인 접근, 고의적인 파괴 및 변경을 방지하고 우발적인 사고로부터 정보를 보호하는 데 있다. 즉, 데이터베

* 본 연구는 정보통신부의 대학 S/W 연구 센터 지원사업의 연구결과임
** 인하대학교 전자계산공학과(g9731513@inhavision.inha.ac.kr, hybae@inha.ac.kr)
*** 단국대학교 전자계산학과(jdlee@cs.dankook.ac.kr)
**** 선문대학교 산업공학과(rim@omega.sunmoon.ac.kr)

이스 관리 시스템은 데이터베이스에 저장되어 있는 데이터에 대한 불법적인 접근, 고의적인 파괴, 변경, 그리고 비일관성을 발생시키는 접근으로부터 데이터를 보호하기 위하여 보안정책을 수행하여야 한다.[8,11] 예를 들면 미 국방부의 강제적 보안(다단계 보안) 정책은 인가된 개인에 따라 비밀정보의 접근을 제한한다. 비밀 데이터는 비권한 사용자로부터 직접 접근을 보호해야 할뿐 만 아니라, 추론과 같은 간접 수단을 통한 유출을 보호하는 것이 강제적 보안에서는 요구된다.

대부분의 상용 데이터베이스 시스템은 보안 대책으로 데이터에 대한 사용자의 사용 권한을 제어하는 접근 제어(access control)를 채택하고 있으나 이들은 운영 체제를 위한 보안 요구 사항을 반영한 것으로 데이터베이스에 대해서는 적용이 부적합하거나 많은 제약사항을 유발하는 문제점을 지니고 있다.[2,6,9] 데이터베이스 보안을 위한 정책은 크게 임의적 접근 제어(discretionary access control, DAC)와 강제적 접근 제어(mandatory access control, MAC)로 구분된다.[5,11,13] 임의적 접근 제어는 주체(subject)나 주체가 속해 있는 그룹의 식별자를 근거로 객체(object)에 대한 접근을 제한하는 방식이며, 강제적 접근 제어는 객체에 포함된 정보의 비밀 등급(sensitivity)과 주체에 부여된 비밀 취급 인가(authorization 혹은 clearance)를 기반으로 객체에 대한 접근을 제어하는 방식이다. 이는 다단계 데이터베이스 보안 시스템의 주된 제어 방식으로 각 시스템의 주체와 객체에게 보안 등급(security level)을 부여하고, 등급별로 분리된 정보가 하위 등급으로 흘러 내려가는 것을 방지하는 보안 시스템이다.[14] 강제적 보안은 다단계 보안(multi-level security)을 구현하기 위한 방법론의 핵심이 된다.[22]

공간 데이터베이스 시스템(spatial database system)에서의 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. 이를 방지하는 방안은 다양한 방법이 있을 수 있으나, 본 논문에서는 공간 데이터베이스 상에서의 보안 방법을 제공한다. 현재까지 데이터베이스의 보안을 위한 연구들이 많은 부분에서 이루어지고 있지만 공간 데이터베이스를 위한 보안에 대한 연구는 거의 이루어지고 있지 않다. 기존의 관계형 모델은 모델 자체가 표준화되어 있어 사용이 용이하고, 관계형 데이터베이스 관리 시스템에서 제공하는 회복, 보안, 무결성 제어 등의 기능을 활용할 수 있으며, 응용 프로그램의 개발이 용이하다는 장점을 갖는다. 그러나 공간 데이터베이스를 위해 관계형 모델을 적용하는 경우 공간 데이터와 비공간 데이터를 동시에 다루기 때문에 관계형 데이터 모델에서 다루던 튜플이나 필드 수준에서의 다단계 보안 정책으로는 이를 관리가 어렵다. 이는 관계형 데이터 모델을 이용하여 공간 데이터를 표현할 때의 문제는 공간 데이터 타입이 없기 때문에 반드시 문자형이나 숫자를 이용하여 공간 데이터를 표현하여야 하며, 아크와 폴리곤은 테이블 내에 반복되는 식별자와 다수의 튜플로 구성하여야 한다. 공간 데이터 표현에 따른 데이터의 중복성과 데이터의 불일치성 발생 그리고 공간 연산에 대한 효과적인 지원이 어렵다는 문제점을 갖는다. 따라서 이를 위한 정보 테이블을 두어 공간 데이터 처리 부분과 비공간 데이터 처리 부분을 명백히 분리하고 시스템 구조의 복잡성을 줄이며 계층화된 관리를 가능하도록 한다. 그리고 공간 데이터와 비공간 데이터에 대한 보안 등급을 동일하게 유지하여 관리를 용이하게 한다. 이는 권한이 다른 사용자가 공간 데이터는 다루지만 비공간 데이터를 다루지 못하는 불합리함을 해결하도록 한다. 이를 위해 본 논문에서는 다단계 보안 공간 데이터 모델인 MLS/SRDM을 제안한다.

대부분의 공간 데이터베이스는 위상 구조를 갖는 다양한 공간 데이터베이스 시스템에서는 동종의 공간 데이터와 서로 인접한 이종의 공간 데이터를 이용하여 다양한 공간 분석을 수행하여야 하는 특징을 가지며 또한 빠른 공간 분석 수행을 요구한다.[18] 이러한 공간 분석을 효율적으로 수행하기 위해서는 위상 정보의 이용이 필수적이다.

그러나, 공간 데이터베이스를 갖는 지리정보시스템의 경우 대부분의 응용업무가 그래픽 사용자 인터페이스를 사용하고 있기 때문에 기밀이 요구되어지는 공간 데이터베이스의 경우, 출력되어진 객체들의 위치 정보나 인접한 객체와의 위상관계를 통해서 많은 정보가 노출되어질 위험이 있으므로 엄격한 사용자의 접근제어가 요구되어진다. 즉, 공간 데이터베이스에서 공간 데이터간의 위상 정보를 지원하는 경우 위상관계에 의한 정보의 노출이 문제가 된다. 공간 데이터의 경우 비공간 데이터와는 달리 위치 정보를 가지고 있으며 주변의 인접한 객체들과의 위상

관계가 중요한 요소로서 작용한다. 이러한 인접 객체와의 위상관계를 통해서 상위 보안등급 객체에 대한 정보의 대략적인 유추가 가능하다. 즉, 공간 객체단위의 접근 제어를 적용하는 경우 인접 객체들 사이의 위상관계에 의한 기밀한 공간 데이터의 비밀 위상 경로(covert topology channel)로 인한 정보 유출이라는 문제가 발생한다. 이러한 비밀 경로 문제를 해결하기 위해 본 논문에서는 공간 데이터의 위상관계로 인한 정보 유출을 방지하기 위해서 공간 다중인스턴스(polyinstantiation for spatial data)를 제안한다.

II. 다단계 보안 모델

2.1 Bell-LaPadula 모델

다단계 보안 모델에서는 모든 데이터와 사용자에게 보안등급을 부여한다. 사용자 s의 보안등급을 L(s), 데이터 o의 보안등급을 L(o)로 표시하는데, 보안등급은 두 가지의 구성요소 〈레벨(sensitivity level), 범주(categories)〉로 이루어진다. 이 때, 데이터와 사용자에게 부여하는 레벨을 각각 분류(classification), 허용(clearance) 레벨이라 한다. 데이터베이스 시스템이 다양한 보안등급을 가진 정보를 포함하고 가장 높은 보안등급의 데이터를 접근이 불가능한 사용자가 있을 때 다단계의 보안 필요성이 있다. 보안 등급은 *Unclassified*(*U*) 〈 *Confidential*(*C*) 〈 *Secret*(*S*) 〈 *Top Secret*(*TS*)로 나누어진다. 사용자에게 할당된 보안등급은 기밀 정보를 유출하지 않을 사용자의 신뢰도를 반영한다. 다단계 데이터베이스 시스템은 다양한 보안등급을 가지는 데이터와 인가등급을 가지는 사용자를 유지하여야 한다. 가장 일반적인 경우라면 데이터베이스의 원자적 사실(fact)에 각각 보안등급을 부여하는 것이다. 이는 데이터의 접근 등급과 접근을 요청하는 주체의 접근 권한에 따라 데이터의 직접 혹은 간접적인 접근을 통제하는 능력을 의미한다. 이 요구사항은 다음과 같이 형식화될 수 있다. 우선, 모든 가능한 접근 등급의 집합은 지배(dominant)라고 불리는 부분 순서 관계(partial ordering relation) ≥ 를 갖는 래티스(lattice)로써 구조화된다.[4] 그리고 각 주체 s는 읽기를 위한 판독 권한 read-class(s)와 쓰기를 위한 기록 권한 write-class(s)의 두 가지 접근 등급을 갖는다. 이 때 read-class(s) ≥ write-class(s)의 지배 관계가 성립된다. 마지막으로, 인가되지 않는 노출과 파괴로부터 데이터를 보호하기 위하여 강제적 접근제어의 요구조건은 두 가지 규칙으로 형식화된다. 이는 Bell-LaPadula의 강제적 보안정책에 기반을 두고 있다.[10]

(1) 단순 보안 속성 : 주체 s는 접근 등급 x를 갖는 데이터에 대하여 read-class(s) ≥ x의 관계가 성립되지 않는 한 데이터를 읽을 수 없다.
(2) 제한 *-속성 : 주체 s는 접근 등급 x를 갖는 데이터에 대하여 write-class(s) = x의 관계가 성립되지 않는 한 데이터를 기록할 수 없다.

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. 즉, 두 가지 규칙에서 전자는 "no read up", 후자는 "no write down"규칙을 의미한다. 본 규칙을 데이터베이스 환경에서 준수하기 위해서는 SeaView 모델에서 소개한 다중인스턴스화(polyinstantiation) 기법을 사용한다.[3]

2.2 다중인스턴스화

다중인스턴스화는 같은 이름으로 많은 데이터 객체의 동시 존재를 의미한다. 여기서 많은 인스턴스화들은 그들의 보안등급으로 구별된다. 이는 다단계 보안의 불가피한 결과이고 데이터베이스, 릴레이션, 튜플 그리고 데이터 속성값에 영향을 준다.[20]

(1) 다중인스턴스화 릴레이션(PIR)들은 릴레이션 이름 R과 스키마 보안등급(R)에 의해 구별되는 릴레이션들이다. 그래서 동일 이름 R이지만 다른 class(R)을 가진 몇 개의 릴레이션들이 존재할 수 있다.
(2) 다중인스턴스화 튜플(PIT)들은 주키와 관련키 보안등급에 의해 구별되는 튜플이다. 그래서 같은 다단계 릴레이션에는 주키 값은 같지만 서로 다른 보안등급인 몇 개의 튜플 인스턴스들을 포함할 수 있다.
(3) 다중인스턴스화 속성값(PIE)들은 주키, 키 보안등급, 그리고 속성값 보안등급에 의해 구별되는

Mission

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

〔그림 1〕 다중인스턴스화의 예

속성값들이다. 그래서 다른 보안등급이지만 같은 〔주키, 키 보안등급〕의 쌍과 연관되는 속성에 대하여 많은 속성값들이 존재할 수 있다.

다중인스턴스화은 다단계 릴레이션, 강제적 보안, 여과의 자연스러운 결과이다. 다중인스턴스화 데이터를 주체가 완전히 알아채지 못하는 방법으로 다중인스턴스화를 유지해야 한다. 다음 〔그림 1〕은 다중인스턴스화의 예를 보여준다.

Ⅲ. MLS/SRDM : 다단계 공간 데이터 모델

본 논문에서는 다단계 보안을 지원하기 위하여 기존의 공간 관계 데이터 모델(Spatial Relational Data Model)을[7,12,15] 확장한 MLS/SRDM(Multi Level Security/Spatial Relational Data Model)을 기반으로 한다. MLS/SRDM은 공간 데이터베이스 설계 단계에서 다단계 보안을 정의하는 데이터 모델이다. 즉, 데이터베이스 관리 시스템과 독립적인 데이터 모델로 공간 데이터를 위한 객체 표현과 비공간 데이터를 위한 관계 표현을 이용하여 공간 객체 단계에 대해 다단계 보안을 지원하는 구조로 구성하여 설계한다.

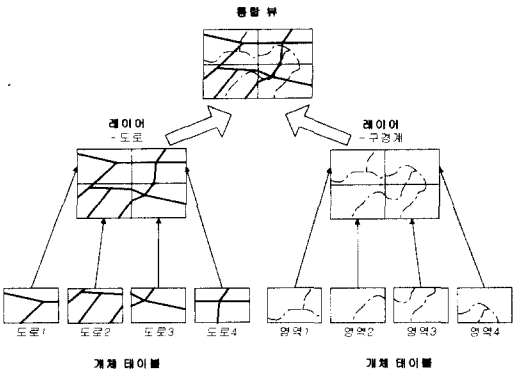
SRDM은 객체 표현과 관계 표현을 이용하여 공간 객체를 상위 단계에서 계층 구조로 구성하여 공간 데이터와 비공간 데이터를 통합 관리할 수 있는 다단계 데이터 모델이다.[19] 이는 공간 객체에 대한 다양한 표현 및 사용자 관점에서의 논리적인 단위를 제공하기 위한 개념 단계 모델과 하위 단계에서 실제로 저장 공간에 표현되며 공간 객체에 대한 효율적인 처리가 가능한 구현 단계 모델로 나누어 구성한다. 개념 단계 모델은 상위 단계에서 사용자 관점에서 다루어지는 공간 객체의 집합으로 표현되고, 하위 단계에서는 개개의 공간 객체에 대한 타입별로 표현된다. 구현 단계 모델은 공간 객체에 대한 실제 저장 표현을 나타내며 공간 객체에 대한 효율적인 공간 연산을 처리할 수 있도록 구성한다.

3.1 MLS/SRDM의 개념 단계 모델

MLS/SRDM은 공간 객체와 이와 연관된 비공간 데이터에 대한 논리적인 다단계 과정을 통하여 공간 데이터와 비공간 데이터에 대한 효과적인 보안을 지원할 수 있도록 설계한다.

공간 데이터의 다단계 보안을 지원하기 위한 데이터 모델에 대한 고려 사항은 우선 시스템 관점에서 공간 객체에 대한 다단계 보안 표현의 용이성과 다양성을 제공하여야 한다는 것과 구현 단계에서 모델링에 대한 효율적인 처리 및 표현이 가능하여야 한다는 것이다.

본 논문에서 제안하는 다단계 보안 공간 데이터 모델인 MLS/SRDM은 다단계 구조 모델(layered architecture model)로 구성되며 SRDM의 구조와 마찬가지로 개념 단계 및 내부 단계로 구분된다. 개념 단계는 관리자 단계로 통합된 공간 객체의 논리적인 구조와 보안에 대한 표현 단계이고, 내부 단계는 실제로 물리적인 저장 공간에 표현되는 단계이다. 이러한 다단계 구조는 공간 객체간의 다단계 과정을 통하여 각 단계별 데이터와 접근 방식에 대해 독립성을 유지하므로 기존의 공간 데이터베이스 시스템의 자원을 그대로 사용할 수 있으며 구현 단계에서 보안을 지원하는 것이 용이하다. 반면 각 단계간에 필요한 통신의 부하가 상당하여 성능 저하를 유발할 수 있으며 보안 검증을 위한 상호 작용에 대해 동시성 제어나 인증 요소가 지원되지 않는 이질성이 유발할 수도 있다.[17] 〔그림 2〕는 MLS/SRDM의 개념 단계 모델을 보여준다.

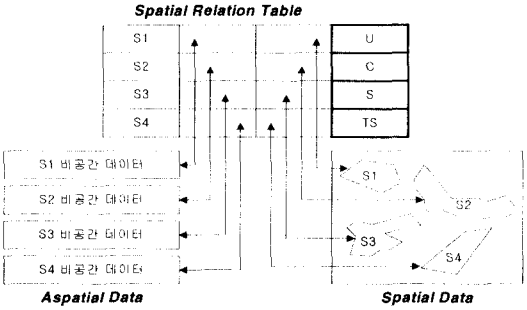


〔그림 2〕 MLS/SRDM의 개념 단계 모델

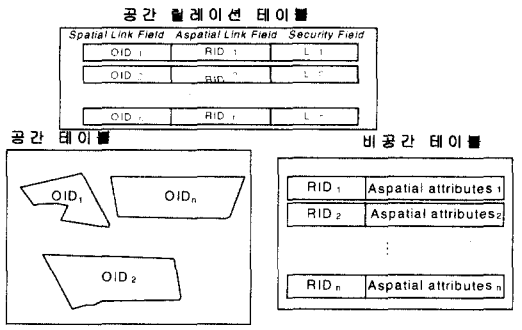
3.2 MLS/SRDM의 구현 단계 모델

공간 데이터와 비공간 데이터를 통합 관리하기 위한 단계로 공간 데이터와 비공간 데이터의 연관성을 부여하기 위한 연결 방법은 전진 연결 방법과 후진 연결 방법이 있으며, 이를 혼합한 양방향 연결 방법도 있다.[21] 제안 시스템에서는 [그림 3]과 같이 공간 객체를 공간 릴레이션 테이블(Spatial Relation Table), 공간 테이블(Spatial Table) 그리고 비공간 테이블(Aspatial Table)의 다단계의 계층으로 구성하는 양방향 연결 방법을 사용한다.

이는 공간 데이터 처리 부분과 비공간 데이터 처리 부분을 명백히 분리하여 시스템 구조의 복잡성을 줄이며 계층화된 관리를 가능하게 한다. 그리고 공간 데이터와 비공간 데이터에 대한 보안 등급을 같이 유지하여 관리를 용이하게 한다. 또한 공간 객체의 관리를 항상 공간 릴레이션 테이블을 통하여 이루어지도록 하여 공간 데이터와 비공간 데이터간의 무결성을 유지한다. 이는 권한이 다른 사용자가 공간 데이터는 다루지만 비공간 데이터를 다루지 못하는 불합리함을 해결하도록 한다. [그림 4]는 MLS/SRDM에서의 공간 릴레이션 테이블, 공간 테이블 그리고 비공간 테이블로 구성된 구체적인 다단계의 계층 구조를 나타낸다.



[그림 3] MLS/SRDM의 구현 단계 모델



[그림 4] 공간 객체의 테이블 표현에 대한 다단계 보안

(1) 공간 릴레이션 테이블

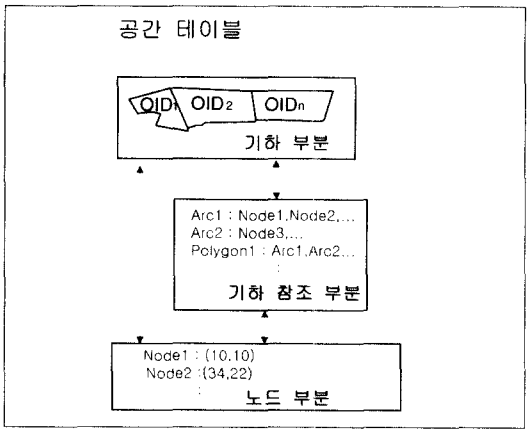
공간 릴레이션 테이블(Spatial Relation Table)은 공간 데이터와 비공간 데이터의 연결을 이루고 있는 부분과 다단계 보안등급을 갖는 필드로 구성된다. 공간데이터와 비공간 데이터를 연결하기 위해서 공간 연결 필드(Spatial Link Field)와 비공간 연결 필드(Aspatial Link Field)를 갖는다. 공간 연결 필드는 공간 테이블의 객체 식별자(Object IDentifier : OID)를 갖고, 비공간 연결 필드는 비공간 테이블의 레코드 식별자(Record IDentifier : RID)를 갖는다. 그리고 보안등급필드(Security Field)는 공간 데이터와 비공간 데이터의 동일한 보안등급을 갖는다.

(2) 공간 테이블

공간 테이블(Spatial Table)은 공간 데이터를 저장하며, 위상 관계의 표현과 공간 데이터의 무결성을 유지하기 위하여 [그림 5]와 같이 기하 부분(Geometric Part), 기하 참조 부분(Geometric Reference Part), 그리고 노드 부분(Node Part)의 세 단계로 나누어 표현한다.

기하 부분은 독립적인 공간 데이터를 저장하는 부분으로 공간 릴레이션 테이블로부터 직접 연결된다. 기하 부분에는 기하 참조 부분 또는 노드 부분에서 정의된 공간 데이터와 공간 데이터의 형태 속성값인 색깔, 선 종류, 채움 형식 등을 갖는다.

기하 참조 부분은 기하 부분에서 참조되고 있는 중간 형태의 공간 데이터 즉 위상 정보를 갖는 데이터들에 대한 정보를 저장하며, 기하 참조 부분 또는 노드 부분에서 정의된 공간 데이터를 지칭한다. 기하 참조 부분에서 정의된 중간 형태의 공간 데이터



[그림 5] 공간 테이블의 다단계 표현

는 무결성을 보장하기 위하여 단독으로 삭제될 수 없으며, 공간 데이터의 형태 속성은 갖지 않는다.

노드 부분은 각각의 공간 데이터에 대한 실제 좌표값이 저장되며, 위상 레벨을 갖는 경우 기하 참조 부분과 함께 위상 정보로써의 역할을 수행한다.

(3) 비공간 테이블

비공간 테이블(Aspatial Table)은 속성 데이터인 비공간 데이터를 저장하는 부분으로 튜플 형식의 일반 테이블의 구조로 관리된다. 여기에는 공간 데이터와 연결하기 위한 레코드 식별자를 갖고 있으며, 외부 데이터베이스 관리 시스템을 사용할 경우에는 비공간 테이블은 존재하지 않으며 데이터베이스 관리 시스템에서 관리되는 주키 값이 공간 릴레이션 테이블에 레코드 식별자로 저장된다.

3.3 MLS/SRDM의 모델 구성 요소

MLS/SRDM에서 제안하는 공간 클래스와 구성 요소 즉, 공간 테이블, 비공간 테이블, 공간 릴레이션 테이블과 이에 대한 보안등급을 정의하면 다음과 같다.

[정의 1] 공간 클래스

$S=(OID, G, T)$
OID // 공간 객체의 ID
$G=\{P, L, R\}$ // 공간 기하 클래스
$T=\{TN, TA, TP\}$ // 공간 위상 클래스

공간 데이터베이스 시스템을 위한 공간 데이터 타입으로는 점, 선, 영역 데이터의 기하 클래스뿐만 아니라 이들을 계층적으로 결합하여 새로운 사용자 데이터 타입을 제공할 수 있도록 복합 데이터 타입인 위상 클래스를 포함한다. 이러한 위상 클래스는 기하 클래스가 갖는 논리적인 데이터 구조로 각 데이터를 인스탄스로 간주하며 자신은 복합 데이터 타입을 대표로 표현하는 통합 객체 데이터로 간주된다.

[정의 2] 공간 기하 클래스

$G=\{P, L, R\}$
$P=\{P_1, P_2, \cdots, P_n\}$ // 공간기하클래스의 점 집합
$L=\{L_1, L_2, \cdots, L_n\}$ // 공간 기하 클래스의 선 집합
$R=\{R_1, R_2, \cdots, R_n\}$ // 공간 기하 클래스의 면 집합

공간 데이터 타입의 기본 타입인 기하 클래스는 점, 선, 영역 데이터 타입으로 구분되며 다음과 같이 P, L, R 클래스를 정의한다.

- 유클리드 기하 평면(Euclidean plan) R^2에 대하여 점 데이터를 위한 하나의 좌표 값을 갖는 클래스를 P 클래스라 한다.
- 유클리드 기하 평면 R^2에 대하여 선 데이터를 위한 두 개 이상의 P 클래스와 그들 사이에 연결된 선분으로 구성된 클래스를 L 클래스라 한다.
- 유클리드 기하 평면 R^2에 대하여 영역 데이터를 위한 세 개 이상의 L 클래스에 대하여 그가 구성하는 처음 L 클래스의 시작 P 클래스 값과 마지막 L 클래스의 끝 P 클래스의 값이 동일하고, 그들이 둘러싸고 있는 내부 영역으로 구성된 클래스를 R 클래스라 한다.

[정의 3] 공간 위상 클래스

$T=\{TN, TA, TP\}$
$TN=\{N_1\}$ // P 클래스로 인한 노드 데이터
$TA=\{N_1, N_2, \cdots, N_n\}$ // L 클래스로 인한 아크 데이터
$TP=\{N_1, N_2, \cdots, N_1\}$ // 폐합된 영역을 생성하는 폴리곤 데이터

공간 객체의 위상을 표현하기 위해서 기하 클래스인 점, 선, 영역 데이터 타입으로부터 위상 클래스 T를 정의한다.

- 유클리드 기하 평면 R^2에 대하여 노드 데이터를 위한 하나의 P 클래스와 식별자로 구성된 클래스를 TN 클래스라 한다.
- 유클리드 기하 평면 R^2에 대하여 아크 데이터를 위한 하나의 식별자와 두 개 이상의 TN 클래스 집합, 그리고 그들 사이에 연결된 선분으로 구성된 클래스를 TA 클래스라 한다.
- 유클리드 기하 평면 R^2에 대하여 폴리곤 데이터를 위한 하나의 식별자와 세 개 이상의 TA 클래스의 집합에 대하여 그가 구성하는 처음 TA 클래스의 시작 TN 클래스 값과 마지막 TA 클래스의 끝 TN 클래스의 값이 동일하고, 그들이 둘러쌓고 있는 내부 영역으로 구성된 클래스를 TP 클래스라 한다.

〔정의 4〕 비공간 테이블

$A=(RID, Ac)$

RID // 비공간 테이블의 ID

$Ac=\{A_1, A_2, \cdots, A_n\}$ // 속성 어트리뷰트의 집합

비공간 테이블은 관계형 모델의 스키마처럼 튜플 형식의 일반 테이블의 구조로 관리된다. 공간 데이터와 연결하기 위한 레코드 식별자를 갖고 있다.

〔정의 5〕 공간 릴레이션 테이블

$SA=(OID, RID, L)$

OID // 공간 객체의 ID

RID // 비공간 테이블의 ID

L // 공간객체와 비공간 테이블의 보안 등급

공간 릴레이션 테이블 SA는 공간 데이터와 비공간 데이터의 연결을 이루고 있는 부분과 다단계 보안등급을 갖는 필드로 구성된다. 공간 데이터와 비공간 데이터를 연결하기 위해서 공간 테이블의 객체 식별자와 비공간 테이블의 레코드 식별자를 갖는다. 그리고 보안등급 필드는 공간 데이터와 비공간 데이터의 동일한 보안등급을 갖는다.

〔정의 6〕 보안 등급

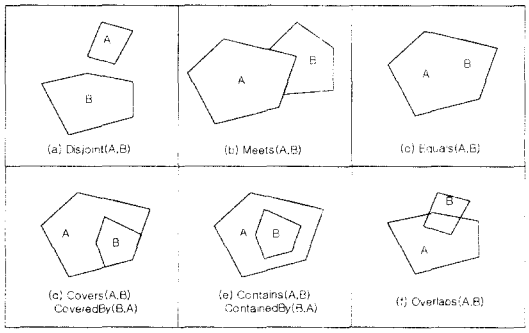
$L=\langle l, h\rangle \subseteq \{U, C, S, TS\}$

보안 등급의 전체 집합은 L={U, C, S, TS} 이며 전체 순서 U(Unclassified) 〈 C(Confidential) 〈 S(Secret) 〈 TS(Top Secret)를 갖는다. 보안 등급 L은 〈l, h〉로 표현되며, L의 부분 순서 집합이다. l 은 보안 등급의 하한(lower bound)이고 h 는 보안 등급의 상한(upper bound)이다.

Ⅳ. 비밀 위상 경로를 해결하는 공간 다중 인스턴스화

4.1 공간 위상 연산

공간 데이터베이스 시스템을 위한 다양한 공간 연산 중에서 위상 데이터에 대한 효율적인 처리를 지원하는 위상 연산이 있다. 이러한 위상 구조를 갖는 다양한 공간 데이터베이스 시스템에서는 동종의 공간 데이터와 서로 인접한 이종의 공간 데이터를 이용하여 다양한 공간 분석을 수행하여야 하는 특징을 가지며 또한 빠른 공간 분석 수행을 요구한다. 이러한 공간 분석을 효율적으로 수행하기 위해서는 위상 정보의 이용이 필수적이다.[1,16]



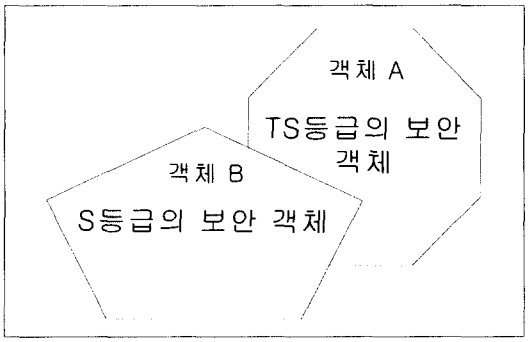
〔그림 6〕 영역 데이터에 대한 각 위상 관계 연산의 예

위상 연산은 공간 객체로부터 상호 관련성을 찾아내는 연산으로 여기에는 위상 구조를 갖지 않는 기하 데이터 타입으로부터 위상 정보를 생성하는 위상 생성 연산과 두 공간 객체간의 관계를 표현하는 위상 관계 연산 그리고 두 공간 객체로부터 집합 연산을 통하여 새로운 공간 객체를 생성하는 위상 추출 연산으로 나뉜다.

이 때 위상 관계 연산은 두 공간 데이터간의 관련성을 참(true) 또는 거짓(false)의 논리값으로 반환하는 연산으로 여기에는 두 공간 데이터간의 Disjoint, Meets, Equals, Covers, CoveredBy, Contains, ContainedBy, Overlaps 등의 8가지 관계를 나타낸다. 〔그림 6〕은 영역 데이터에 대한 각 위상 관계 연산의 예이다.

4.2 비밀 위상 경로

공간 데이터베이스에서 공간 데이터간의 위상 정보를 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 〔그림 7〕에서 S등급의 사용자가 객체 A(TS등급)는 객체 B(S등급)의 북동쪽에 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.



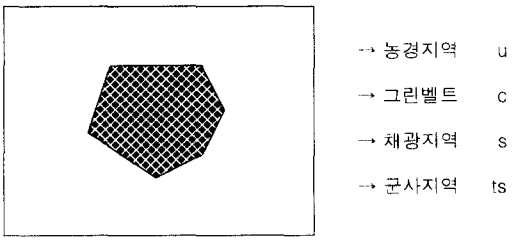
[그림 7] 공간 객체의 위상 관계에 의한 노출

또한, 공간 데이터베이스의 경우 대부분의 어플리케이션들이 그래픽 유저 인터페이스를 사용하고 있기 때문에 기밀이 요구되어지는 공간 데이터베이스의 경우 공간 객체들의 위치정보나 인접한 객체와의 위상관계를 통해서 많은 정보가 노출되는 위험이 있다. 즉, 이러한 공간 객체단위의 접근 제어를 적용하는 경우 인접 객체들 사이의 위상관계에 의한 기밀한 공간 데이터의 비밀 위상 경로(covert topology channel)로 인한 정보 유출이라는 문제가 발생한다.

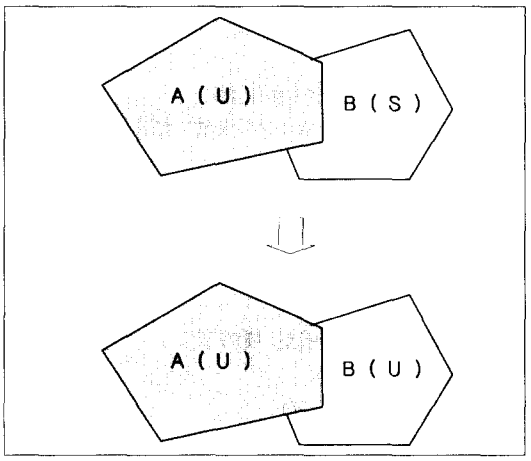
4.3 공간 다중인스턴스화

공간 다중인스턴스화(polyinstantiation for spatial data)는 공간 데이터베이스에서 보안 등급이 다른 사용자들로 하여금 단일 공간 객체에 대해 서로 다른 공간 객체를 가지도록 할 때 발생한다. 공간 데이터베이스 시스템에서의 서로 다른 권한을 가진 사용자는 동일한 공간 객체에 대해 상이한 공간 객체 값을 가질 수 있다. 다음 [그림 8]은 다른 보안 등급을 갖는 공간 다중인스턴스의 예이다.

공간 객체가 보안등급 TS를 갖는다는 것은 이 객체의 존재등급이 TS라는 것을 의미한다. 이 때 이 공간 객체를 접근할 수 있는 사용자는 TS 보안등급을 가지고 있어야 한다.



[그림 8] 공간 다중인스턴스의 예



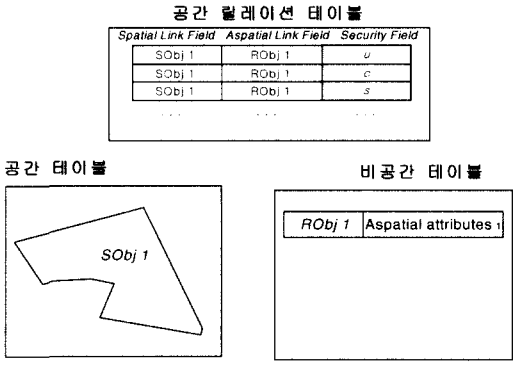
[그림 9] 공간 다중인스턴스의 표현

다음은 공간 다중인스턴스화의 예를 보여준다. "A마을에 인접한 주제별 지역을 검색하시오."라는 공간 질의가 있을 경우 다단계 보안을 제공하는 공간 데이터베이스 시스템은 이에 적합한 보안처리를 해 주어야 한다. 예를 들어 A마을 동쪽에 상수도 보호 지역이 있을 경우 낮은 등급의 사용자에게 상수도 보호지역의 보안이 제공되어져야 한다. 즉, 상수도 보호 지역 접근 등급이 주체(사용자)보다 높을 경우 본 주체는 이 지역의 위치를 검색하거나 추론할 수 없도록 해야 한다. 이러한 문제를 해결하기 위해 본 시스템에서는 공간 다중인스턴스를 제공한다.

[그림 9]에서 공간 객체 A와 공간 객체 B에 대한 인접 연산이 행하여 질 경우 공간 객체 B의 보안 등급(S)이 높기 때문에 공간 객체 B, 즉 '상수도 보호 지역'의 보안 정보가 낮은 등급(U)의 공간 객체로 정보가 흐르는 비밀 경로가 발생한다. 이를 방지하기 위해 다음 4.4에서 제안하는 알고리즘을 이용하여 강제적으로 공간 객체 B의 등급을 S에서 U로 변경한다. 이를 통해 보안등급이 공간 객체 A에서 공간 객체 B로 정보가 흘러가는 것을 방지한다.

4.4 공간 다중인스턴스의 저장 구조

본 논문에서는 동일한 공간 객체에 대하여 상이한 접근등급을 공간 객체 값 다중 인스턴스를 갖는 다중 인스턴스화 튜플(PIT)기법을 이용한다. 이는 공간 릴레이션 테이블을 확장하여 관리하도록 한다. 다음 [그림 10]은 공간 다중 인스턴스를 위한 공간 릴레이션 테이블의 확장이다. 공간 릴레이션 테이블의 튜플은 공간 객체 ID와 비공간 객체 ID의 복합키이다.



〔그림 10〕 공간 다중 인스턴스를 위한 공간 릴레이션 테이블

공간 릴레이션 테이블은 상이한 접근 등급을 갖는 공간 다중인스턴스를 위해 다수의 튜플을 가질 수 있다.

4.5 공간 다중인스턴스화 알고리즘

본 논문에서 제안하는 위상 정보를 위한 데이터 구조는 위상 구조를 단계별로 생성하여 구분된 레이어 단위로 공간 데이터베이스를 관리한다. 또한 기본 클래스인 점, 선, 영역 데이터 타입으로부터 각 공간 객체간의 연결성, 인접성 및 포함성 등의 위상 정보를 생성하여 저장, 관리한다. 이로써 위상 연산에 대해 빠른 질의 처리를 수행하도록 한다.
이 때, 공간 객체의 위상 관계로 인한 정보의 노출을 방지하기 위해 공간 다중인스턴스화를 위한 알고리즘을 제안한다.

다음 〔알고리즘 1〕은 임의의 두 공간 데이터에 대한 포함관계를 구하는 알고리즘으로 공간 데이터 S1의 모든 정점들이 공간 데이터 S2에 포함되어 있는지를 비교한다. 그리고 S1의 보안등급 L1, S2의 보안등급 L2를 비교하여 비밀경로를 방지하기 위해 높은 등급의 객체에 대한 보안등급을 변경한다.

공간함수 CONTAIN은 다각형 즉, 영역과 점과의 관계로 점이 영역 안에 포함되어 있는 지의 여부를 판단한다. 검사할 점에서 아래로 내린 수선과 다각형의 변이 만나는 횟수로 포함 관계를 결정한다. 즉 아래로 내린 수선이 영역과 홀수 번 만나면 주어진 점은 영역에 포함되어 있는 것이고 짝수 번 만나면 포함되지 않은 것이다. 그리고 두 공간 객체의 보안등급을 검색하여 포함관계가 결정한 후 이를 토대로 공간 다중인스턴스화를 수행한다.

〔알고리즘 1〕 *CONTAIN(S1, L1, S2, L2)*

Input : Spatial Data(S1), Security Level(L1), Spatial Data(S2), Security Level(L2)
Output : if S1 contains S2, TRUE else FALSE

```
bool CONTAIN(S1, L1, S2, L2)
{
 T=0
 K is the number of points of S1
 for each point p in S1
    if (p is the on the line S2)
          T=T+1
    else {
      p_ver is a virtual line to p
      if a number of vertex intersections
        between p_ver and S2 are odd then
T=T+1
    }
    if (T==K ) {
       if (L1=>L2) {L1=L2 else L2=L1
            return TRUE
       } else return FALSE
}
```

다음 〔알고리즘 2〕은 교차 관계를 위한 알고리즘으로 교차 관계는 공간 데이터가 다른 공간 데이터와 교차하는 지의 여부를 구하는 것이다. 임의의 두 공간 데이터에 대한 교차 관계는 공간 데이터 S1의 임의의 한 선분이라도 공간 데이터 S2의 어떤 선분과 교차하게 되면 TURE을 반환하는 기능을 수행한다. 그리고 S1의 보안등급 L1, S2의 보안등급 L2를 비교하여 비밀경로를 방지하기 위해 높은 등급의 객체에 대한 보안등급을 변경한다.

〔알고리즘 2〕 *INTERSECT(S1, L1, S2, L2)*

Input : Spatial Data(S1), Security Level(L1), Spatial Data(S2), Security Level(L2)
Output : if S1 intersect S2, TRUE else FALSE

```
int interpoint(int ax1, int ay1, int ax2,
int ay2, int bx1, int by1, int bx2, int by2,
int *px, int *py)
{
 int checkbit;
 float k1, k2;
```

```
 k1=(ay2-ay1)/(ax2-ax1);
 k2=(by2-by1)/(bx2-bx1);
 if (ax1==ax2) {*px=ax1; *py=(int)(k2*
(*px-bx1)+by1); }
 else
   if (bx1==bx2) {*px=bx1; *py=(int)(k1*
(*px-ax1)+ay1); }
    else {
     *px=(int)(k1*ax1-k2*bx1-ay1+by1)/(k1-k2);
     *py=(int)(k1*(*px-ax1)+ay1);
    }/* 좌표의 중간 점에 들어 있는가를 검사 후 */
  if (check(px, py)==0) return 0;
  else return 1;
} /* end of interpoint */

bool INTERSECT(S1, L1, S2, L2)
{
for each end points p1, p2 in S1
 for each end points p3, p4 in S2
   if (interpoint(p1.x, p1.y, p2.x, p2.y,
p3.x, p3.y, p4.x, p4.y, &px, &py)==0) {
      if (L1=>L2) {L1=L2 else L2=L1
         return TRUE
      }
   return FALSE
}
```

V. 결 론

데이터베이스 보안의 목적은 권한이 없는 사용자를 제어하여 정보의 불법적인 접근, 고의적인 파괴 및 변경을 방지하고 우발적인 사고로부터 정보를 보호하는 데 있다. 기밀 데이터는 비권한 사용자로부터 직접 접근을 보호해야 할 뿐만 아니라, 추론과 같은 간접 수단을 통한 유출을 보호하는 것이 강제적 보안에서 요구된다.

기밀이 요구되어지는 공간 데이터베이스의 경우, 출력되어진 객체들의 위치 정보나 인접한 객체와의 위상관계를 통해서 많은 정보가 노출되어질 위험이 있으므로 엄격한 사용자의 접근제어가 요구되어진다. 이러한 인접 객체와의 위상관계를 통해서 상위 보안등급 객체에 대한 정보의 대략적인 유추가 가능하다. 이러한 공간 객체단위의 접근 제어를 적용하는 경우 인접 객체들 사이의 위상관계에 의한 기밀한 공간 데이터의 비밀 위상 경로로 인한 정보 유출이라는 문제가 발생한다. 이러한 비밀 경로 문제를 해결하기 위해 본 논문에서는 공간 데이터의 위상관계로 인한 정보 유출을 방지하기 위해서 공간 다중인스턴스화를 제안했다. 그리고 다단계 공간 데이터베이스를 위한 다단계 공간 데이터 모델인 MLS/SRDM을 설계하였다.

이러한 공간 다중인스턴스를 통하여 서로 다른 권한을 가진 사용자는 동일한 공간 객체에 대해 상이한 공간 객체 값을 가질 수 있고 이를 통해 보안등급이 높은 객체에서 낮은 객체로 정보가 흘러가는 것을 방지할 수 있다.

참 고 문 헌

[1] I. Bracken and C. Webster, "Towards a topology of a geographic information systems," *International Journal of Geographic Information Systems*, Vol. 3, No. 2, pp. 137~152, 1989.

[2] J. R. Campbell, "A Brief Tutorial on Trusted Database Management Systems," *Proceedings of 13th National Computer Security and Privacy*, pp. 133~142, May. 1990.

[3] 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.

[4] D. E. Denning, *Cryptography and Data Security*, Addison-Wesley, 1983.

[5] Department of Defense National Computer Security Center, "Department of Defense Trusted Computer System Evaluation Criteria," DoD 5200.28-STD, DoD NCSC, Dec. 1985.

[6] E. B. Fernandez, R. C. Summers and C. Wood, *Database Security and Integrity*, Addison-Wesley, 1981.

[7] O. Gunther, "Efficient Computation of Spatial Joins," *Proceedings of 9th International Conference on Data Engineering*, pp. 50~59, 1993.

[8] S. Jajodia, "Database security : Current

Status and Key Issues," *SIGMOD Record*, Vol. 19, No. 4, pp. 123~126, Dec. 1990.

[9] S. Jajodia and R. S. Sandhu, "Toward a Multilevel Secure Relational Data Model," *Proceedings of ACM SIGMOD International Conference on Management of Data*, pp. 50~59, May. 1991.

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

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

[12] A. Pizano et al., "Specification of Spatial Integrity Constraints in Pictorial Databases," *Computer*, Vol. 22, pp. 59~71, 1989.

[13] R. S. Sandhu, "Mandatory Controls for Database Integrity," *Proceedings of the IFIP WG 11.3 Workshop on Database Security*, pp. 143~150, Sep. 1989.

[14] R. S. Sandhu, Lattice-based access control models, *Computer*, Vol. 26, pp. 9~19, Nov. 1993.

[15] M. Stonebraker, "Implementation of Rules in Relational Data Base Systems," www.cs.berkely.edu, pp. 1~10, 1983.

[16] T. Ubeda and M. F. Egenhofer, "Topological Error Correcting in GIS," *Proceedings of 5th Symposium on Spatial Databases SSD'97*, pp. 283~297, 1997.

[17] J. Widom and S. Ceri, *Active Database Systems: Triggers and Rules for Advanced Database Processing*, Morgan Kaufmann, 1996.

[18] 김영란, 김종훈, 김재홍, 배해영, "공간 세그먼트의 효율적인 공유를 지원하는 위상 자료 구조", *한국정보과학회 학술발표논문집*, 제24권 제1호, 1997.

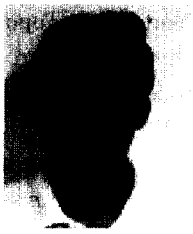
[19] 박상일, 김종훈, 배해영, "공간 데이터베이스 시스템에서의 계층적인 데이터 표현", *한국정보처리학회 학술발표논문집*, 제3권 제1호, 1996.

[20] 이상원, 김형주, "객체지향 데이터모델에서 다중사례화를 위한 버전개념 확장", *한국정보과학회 논문지*, 제21권 제2호, 1994.

[21] 이영걸, 공간 데이터베이스에서 의미적 무결성 관리기의 설계 및 구현, *박사학위논문*, 인하대학교, 1999.

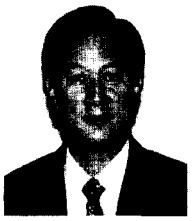
[22] 조완수, 배해영, "다단계 보안을 위한 관계 데이터 모델의 확장", *한국통신정보보호학회 논문지*, 제5권 제3호, 1995.

〈著者紹介〉



오 영 환 (Young-Hwan Oh)
1993년 2월 : 인하대학교 전자계산공학과 졸업
1997년 2월 : 인하대학교 전자계산공학과 석사
1997년 3월~현재 : 인하대학교 전자계산공학과 박사과정
〈관심분야〉 지리정보시스템, 데이터베이스 보안, 정보보호

이 재 동 (Jae-Dong Lee)
1985년 2월 : 인하대학교 전자계산학과(B.S)
1991년 3월 : Cleveland State University(미), 전산정보학(M.S)
1996년 5월 : Kent State University(미), Computer Science(Ph.D)
1985년 7월~1988년 10월 : 대우중공업 정보관리센터
1996년 9월~1997년 2월 : (주) 두루넷 기술기획
1999년 8월~현재 : 지능형 GIS 연구센터 연구위원
1997년 3월~현재 : 단국대학교 전자계산학과 교수
〈관심분야〉 ATM networks, 분산 및 병렬처리, Network computing



임 기 욱 (Kee-Wook Rim)
1977년 2월 : 인하대학교 전자공학과 학사
1987년 2월 : 한양대학교 전자계산학과 석사
1994년 8월 : 인하대학교 전자계산학과 박사
1977년~1983년 : 한국전자기술연구소 선임연구원
1983년~1988년 : 한국전자통신연구소 시스템소프트웨어 연구실장
1988년~1989년 : 미 캘리포니아 주립대학(Irvine) 방문연구원
1989년~1997년 : 한국전자통신연구원 시스템연구부장
주전산기(타이컴) III, IV 개발 사업책임자
1997년~2000년 : 정보통신연구진흥원 정보기술전문위원
2000년~현재 : 선문대학교 산업공학과 교수
〈관심분야〉 데이터베이스시스템, 시스템구조, 운영체계, 실시간DB

배 해 영 (Hae-Young Bae)
1974년 2월 : 인하대학교 응용물리학과 학사
1978년 2월 : 연세대학교 전자계산학과 석사
1989년 2월 : 숭실대학교 전자계산학과 박사
1980년 3월~현재 : 인하대학교 전자계산공학과 교수
1999년 8월~현재 : 인하대학교 지능형 GIS 연구센터장
2000년 6월~현재 : 한국 GIS전문가 협회장
2000년 8월~현재 : 중국 중경우전학원 명예교수
〈관심분야〉 데이터베이스, 멀티미디어DBMS, 지리정보시스템, 실시간DBMS