



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0051919
(43) 공개일자 2009년05월25일

(51) Int. Cl.

H04L 12/24 (2006.01) H04L 12/28 (2006.01)

(21) 출원번호 10-2007-0118378

(22) 출원일자 2007년11월20일

심사청구일자 2007년11월20일

(71) 출원인

고려대학교 산학협력단

서울 성북구 안암동5가1 고려대학교 내

(72) 발명자

이상근

서울 동대문구 제기2동 153 안암골 벽산아파트
101동 203호

고혜경

서울 노원구 월계2동 롯데캐슬루나 121동 1004호

(74) 대리인

현종철

전체 청구항 수 : 총 7 항

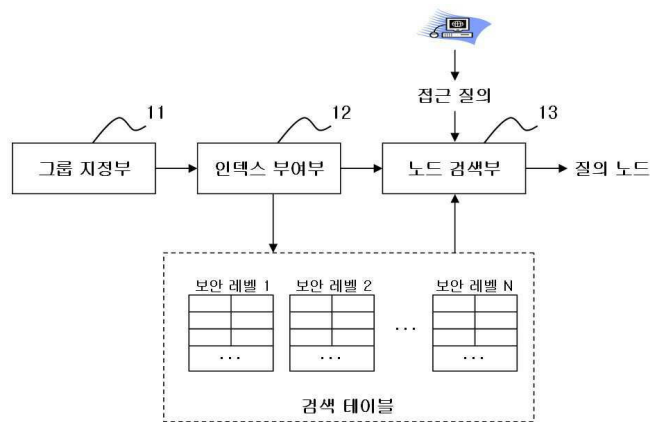
(54) XML 노드에 대한 접근 제어 시스템 및 그 방법

(57) 요약

본 발명은 XML 노드에 대한 접근 제어 시스템 및 그 방법에 관한 것으로, 보다 상세하게는 XML 노드에 대한 접근을 질의한 사용자의 역할별 보안 레벨을 참고하여 XML 노드에 대한 접근 제어를 효율적으로 그리고 안전하게 할 수 있는 시스템 및 방법에 관한 것이다.

본 명세서에서 개시하는 접근 제어 시스템은 다수 XML 노드를 같은 보안 레벨을 가진 것끼리 분류하여 각 그룹으로 지정하는 그룹 지정부; 및 사용자가 상기 다수 노드 중 어느 노드에 대한 접근 질의를 하는 경우, 상기 질의 사용자의 보안 레벨 이하의 노드만을 검색하는 노드 검색부를 포함하여 본 발명의 과제를 해결한다.

대표도 - 도2a



특허청구의 범위

청구항 1

다수 XML 노드를 같은 보안 레벨을 가진 것끼리 분류하여 각 그룹으로 지정하는 그룹 지정부; 및

사용자가 상기 다수 노드 중 어느 노드에 대한 접근 질의를 하는 경우, 상기 질의 사용자의 보안 레벨 이하의 노드만을 검색하는 노드 검색부를 포함하여 상기 질의된 노드에 대한 접근 제어를 하는 XML 노드에 대한 접근 제어 시스템.

청구항 2

제 1 항에 있어서,

상기 각 그룹의 보안 레벨을 각 그룹의 그룹 ID로 지정하고, 상기 다수 노드의 각 노드에 검색 순서를 지정하여 검색 인덱스(index)를 부여하는 인덱스 부여부를 더 포함하는 XML 노드에 대한 접근 제어 시스템.

청구항 3

제 2 항에 있어서,

상기 인덱스 부여부에 의한 검색 순서의 지정은 전위 운행법(preorder traversal)에 의한 것을 특징으로 하는 XML 노드에 대한 접근 제어 시스템.

청구항 4

다수 XML 노드를 같은 보안 레벨을 가진 것끼리 분류하여 각 그룹으로 지정하는 단계; 및

사용자가 상기 다수 노드 중 어느 노드에 대한 접근 질의를 하는 경우, 상기 질의 사용자의 보안 레벨 이하의 노드만을 검색하는 단계를 포함하여 상기 질의된 노드에 대한 접근 제어를 하는 XML 노드에 대한 접근 제어 방법.

청구항 5

제 4 항에 있어서,

상기 각 그룹의 보안 레벨을 각 그룹의 그룹 ID로 지정하고, 상기 다수 노드의 각 노드에 검색 순서를 지정하여 검색 인덱스(index)를 부여하는 단계를 더 포함하는 XML 노드에 대한 접근 제어 방법.

청구항 6

제 5 항에 있어서,

상기 검색 순서의 지정은 전위 운행법(preorder traversal)에 의한 것을 특징으로 하는 XML 노드에 대한 접근 제어 방법.

청구항 7

제 4 항 내지 제 7 항의 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체.

명 세 서

발명의 상세한 설명

기술 분야

<1> 본 발명은 XML 노드에 대한 접근 제어 시스템 및 방법에 관한 것으로, 보다 상세하게는 XML 노드에 대한 접근을 질의한 사용자의 역할별 보안 레벨을 참고하여 XML 노드에 대한 접근 제어를 효율적으로 그리고 안전하게 할 수 있는 시스템 및 방법에 관한 것이다.

배경 기술

- <2> XML(eXtensible Markup Language)은 웹페이지의 구축용 언어인 HTML(Hyper Text Markup Language)을 획기적으로 개선하여 만든 언어로 홈페이지 구축기능, 검색기능 등이 향상되었고 웹페이지의 추가와 작성이 편리해졌으며 클라이언트 시스템의 복잡한 데이터 처리를 쉽게 한다. 이밖에 HTML은 웹 페이지에서 데이터베이스처럼 구조화된 데이터를 지원할 수 없지만 XML은 사용자가 구조화된 데이터베이스를 뜻대로 조작할 수 있는 장점이 있다.
- <3> XML이 웹을 통한 데이터 교환의 표준으로 부각 및 활성화되고 있는 현 시점에서 데이터의 안전한 교환을 위해 XML 데이터를 함유하는 XML 노드에 대한 접근 제어(Access Control) 모델들이 연구되고 있다. 이중 다중 레벨 접근 제어(Multi-level Access Control) 모델은 보안 레벨(security level)에 따라 XML 노드와 사용자에게 서로 다른 접근 제어 규칙을 적용하고 있다.
- <4> 한편 사용자 역할 기반 접근 제어 모델의 경우 사용자의 접근 질의(query)시에 보안 레벨에 따른 정확한 질의 결과를 돌려주기(return) 위해 XML 문서 내에 정의된 동일 명칭의 XML 노드들을 검색한다.
- <5> 그러나 이러한 경우 다음과 같은 문제점이 발생한다.
- <6> 보안 레벨이 사용자 역할 별로 부여된 경우 보안 레벨이 낮은 사용자는 보안 레벨이 높은 노드에 대한 접근이 불허되는데, 노드에 대한 검색은 노드에 설정된 보안 레벨에 관계없이 XML 문서 내에 정의된 동일 명칭의 수많은 노드를 검색하므로 결국에는 사용자의 접근 질의에 대한 처리 속도가 현저히 저하될 수밖에 없으며, 아울러 검색의 필요가 없는 노드에 대한 검색이 이루어지므로 보안상의 안전성을 심각히 훼손할 우려도 발생한다.

발명의 내용

해결 하고자하는 과제

- <7> 본 발명은 상기와 같은 문제점을 해결하기 위해 창안된 것으로, 본 발명이 해결하고자 하는 과제는 XML 노드에 대한 사용자의 접근 질의에 대한 처리를 빠르게 그리고 보안상 안전하게 행할 수 있는 XML 노드에 대한 접근 제어 시스템 및 그 방법을 제공하는 것이다.

과제 해결수단

- <8> 상기와 같은 과제를 해결하기 위해 본 명세서에서 개시하는 XML 노드에 대한 접근 제어 시스템은
- <9> 다수 XML 노드를 같은 보안 레벨을 가진 것끼리 분류하여 각 그룹으로 지정하는 그룹 지정부; 및 사용자가 상기 다수 노드 중 어느 노드에 대한 접근 질의를 하는 경우, 상기 질의 사용자의 보안 레벨 이하의 노드만을 검색하는 노드 검색부를 포함하여 본 발명의 과제를 해결한다.
- <10> 상기와 같은 과제를 해결하기 위해 본 명세서에서 개시하는 XML 노드에 대한 접근 제어 방법은
- <11> 다수 XML 노드를 같은 보안 레벨을 가진 것끼리 분류하여 각 그룹으로 지정하는 단계; 및 사용자가 상기 다수 노드 중 어느 노드에 대한 접근 질의를 하는 경우, 상기 질의 사용자의 보안 레벨 이하의 노드만을 검색하는 단계를 포함하여 본 발명의 과제를 해결한다.

효과

- <12> 본 발명에 의한 XML 노드의 검색은 접근 질의 사용자의 보안 레벨보다 낮은 보안 레벨을 가지는 노드에 대해서만 이루어지므로 접근 질의에 대한 처리 속도를 현저하게 감소시킬 수 있다. 아울러 보다 높은 보안 레벨을 가지는 노드에 대해서는 검색 자체가 이루어지지 아니하므로 불필요한 검색에 따른 보안상의 안전성 훼손의 우려도 방지할 수 있는 부수적 효과도 볼 수 있다.

발명의 실시를 위한 구체적인 내용

- <13> 본 발명에 관한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하고자하는 과제의 해결 방안의 개요를 우선 제시한다.
- <14> 본 발명의 착안점은 보안 레벨이 낮은 사용자의 접근 질의가 있는 경우에 보다 높은 보안 레벨이 설정된 XML 노드에는 접근이 불허되므로, 이러한 사용자가 접근 질의시에는 보안 레벨이 높은 노드에 대한 검색의 필요가 없다는 점이다.

<15> 따라서 보안 레벨이 높은 노드에 대한 검색을 원칙적으로 차단시켜 질의에 대한 처리 속도를 향상시키고 아울러 안전성을 보장하는 검색 방안이 필요한 것인데, 본 발명은 이에 대한 방안을 제시하는 것이다.

<16> 이하, 본 발명의 기술적 과제의 해결 방안을 명확화하기 위한 발명의 구성을 본 발명의 바람직한 실시예에 근거하여 첨부 도면을 참조하여 상세히 설명하되, 도면의 구성요소들에 참조번호를 부여함에 있어서 동일 구성요소에 대해서는 비록 다른 도면상에 있더라도 동일 참조번호를 부여하였으며 당해 도면에 대한 설명시 필요한 경우 다른 도면의 구성요소를 인용할 수 있음을 미리 밝혀둔다.

<17> 다음은 본 발명의 동작을 설명하기 위한 XML 문서의 예시로 병원과 관련된 사용자와 데이터를 그 예로 든 것이다.

```
<hospital>
  <medicalRecords>
    <patient>
      <name>"Tom"</name>
      <wardNo>"456"</wardNo>
      <treatment>...</treatment>
    </patient>
    <patient>
      <name>"Merry"</name>
      <wardNo>"123"</wardNo>
      <treatment>...</treatment>
      <diagnosis>...</diagnosis>
    </patient>
  </medicalRecords>
</hospital>
```

<18> <19> 상기 예시 문서에서 <hospital>, <medicalRecords>, <patient>, <name>, <wardNo>, <treatment>, <diagnosis>가 XML 노드에 해당하며, 'Tom', '456', '123', 'Merry' 는 각 해당 노드의 XML 데이터이다. 한편 <hospital> 노드가 가장 상위 노드에 해당하며, <hospital> 노드의 바로 하위 노드로 <medicalRecords> 노드, <medicalRecords> 노드의 하위 노드로 <patient> 노드가 있다. 그리고 <name>, <wardNo>, <treatment>, <diagnosis> 노드는 <patient> 노드의 하위 노드로 이들은 동위 노드이다. 이때 상, 하위의 개념은 후술할 보안 레벨의 상, 하위를 의미하는 개념과는 다른 의미이다.

<20> 이러한 XML 노드의 구조는 트리(tree) 구조로 표현할 수 있으며 그 트리 구조가 도 1에 제시되어 있다. 트리 구조 표현을 통해 XML 문서의 구조 정보를 한 눈에 파악할 수 있다.

<21> 한편 상기 각 노드에는 보안 레벨(security level)이 설정되는데 보안 레벨의 설정은 XML 데이터의 운전자(위의 예시 문서에 의하면 병원의 운영자가 될 것이다)가 자신의 보안 정책(security policy)에 따라 이루어진다. 이 보안 정책은 결국 각 노드에의 접근 제어의 근간이 되는 것이다.

<22> 한편 다중 레벨 접근 제어 모델에서 보안 등급은 데이터 및 사용자의 성격에 따라 일반적으로 Top secret, secret, confidential, classified, public 등으로 설정될 수 있으며, 레벨이 높은 정도에 5, 4, 3, 2, 1 등의 가중치를 부여하여 순서를 매길 수 있는데, 이 가중치를 보안 레벨로서 활용한다.

<23> 사용자와 XML 문서에 지정된 각 노드들에는 먼저 각각의 보안 레벨을 부여하는데, XML 노드의 경우에는 XML 문서에 보안 레벨을 레이블링(labeling)하여 부여받는다. 레이블링된 XML 문서의 예시가 다음에 제시되어 있다. 이 레이블링된 문서는 위의 예시 문서에 대해 레이블링 작업을 한 문서이다.

```
<hospital p_hospital= "1">
  <medicalRecords p_ medicalRecords= "1" >
    <patient p_patient= "1">
      <name p_name= "1">"Tom"</name>
      <wardNo p_wardNo= "2">"456"</wardNo>
      <treatment p_treatment= "3">...</treatment>
    </patient>
    <patient p_patient= "1">
      <name p_name= "1">"Merry"</name>
      <wardNo p_wardNo= "2">"123"</wardNo>
      <treatment p_treatment= "3">...</treatment>
      <diagnosis p_diagnosis= "3">...</diagnosis>
    </patient>
  </medicalRecords>
</hospital>
```

<24> <25> 이 예시 문서에서 <treatment> 노드와 <diagnosis> 노드의 보안 레벨이 '3' 으로 가장 높게 레이블링 되어 있

다.

- <26> 한편 사용자에게 대한 보안 레벨은 전문의(Specialized Medical Doctor, SMD), 환자(Patient), 병원(Hospital) 3가지로 설정하고 각각의 보안 레벨을 3, 2, 1로 설정한다. 아래 표는 사용자별(역할별) 보안 등급과 보안 레벨을 나타낸다.

사용자(역할)	보안 등급(Security Grade)	보안 레벨(Security Level)
SMD	Top Secret	3
Patient	Secret	2
Hospital	Public	1

- <27>
- <28> 도 2a는 본 시스템 발명의 바람직한 일시예의 구성을 나타낸 도면이며, 도 2b는 본 방법 발명의 바람직한 일시예의 흐름을 제시한 도면이다.
- <29> 그룹 지정부(11)는 XML 문서에 지정된 여러 XML 노드를 보안 레벨 단위로 분류하여 각 그룹으로 지정하는 기능을 수행하는(S21) 부분으로 XML 노드에 대한 보안 레벨의 설정 방식은 상기에서 언급했다. XML 노드를 같은 보안 레벨을 가진 노드들끼리 그룹으로 지정하는 이유는 위에서 언급한 본 발명의 착안점에 기인하는 것이다.
- <30> 노드 검색부(13)는 사용자가 자신이 원하는 XML 데이터를 얻기 위해 XML 노드에 대한 접근 질의를 하는 경우, 그 XML 노드를 검색하는 기능을 수행하는(S23) 부분으로 상기 지정된 각 그룹 중에서 질의 사용자의 보안 레벨 이하인 그룹의 노드만을 검색한다.
- <31> 사용자의 보안 레벨 이하인 그룹의 노드만을 검색하는 이유는 상기한 본 발명의 착안점에서와 같이 역할 기반 접근 제어 모델(다중 레벨 접근 제어 모델)에서는 소정의 보안 레벨을 가진 사용자는 그 자신의 보안 레벨보다 높은 보안 레벨을 가지는 노드에의 접근이 원천적으로 차단되기 때문이다. 접근이 원천적으로 차단되므로 접근의 전체 작업인 검색 절차를 밟을 필요가 없고 따라서 노드 검색부(13)는 질의 사용자의 보안 레벨보다 높은 그룹의 노드에 대한 검색을 스킵(skip)하는 것이다.
- <32> XML 노드에 대한 검색을 수행함에 있어, 그룹만을 참조하여 이루어질 수도 있으나 같은 보안 레벨을 가지는 모든 노드들의 검색 순서를 아울러 정하여 검색을 수행하는 것이 사용자의 접근 질의에 대한 처리 속도를 보다 더 빨리 수행할 수 있다.
- <33> 이를 위해 인덱스 부여부(12)는 각 노드의 보안 레벨을 그룹 ID로 지정하고, 아울러 각 노드에 검색 순서를 지정하여 각 노드에 검색 인덱스(index)를 부여한다. 즉, 각 노드에는 그룹 ID와 검색 순서를 한 쌍으로 하는 고유 검색 인덱스가 부여된다(S22).
- <34> 여기서 검색 순서는 노드 검색시에 노드의 방문 순서를 의미하는 것으로, 도 1에 제시된 바와 같이, XML 노드의 구조는 트리 구조로 표현할 수 있는데 트리 구조로 표현된 노드(데이터)의 방문 순서를 정함에 있어서는 전위 순회법(preorder traversal), 중위 순회법(inorder traversal), 후위 순회법(postorder traversal) 등 여러 방안이 있을 수 있다. 본 발명에서는 전위 순회법을 이용하여 노드의 방문 순서를 정한다.
- <35> 전위 순회법은 부모 노드를 먼저 순회하고 왼쪽 자식 노드, 오른쪽 자식 노드 순으로 순회하는데, 전위 순회법을 이용하면 부모를 근으로 해서 자식 노드로 차례차례 증가하여 순차적으로 레이블을 줄 수 있으며 트리의 왼쪽 트리와 오른쪽 트리를 확연히 구분할 수 있다. 따라서 본 발명은 XML 문서에 정의된 XML 노드의 방문 순서(order)를 부여할 때 전위 순회법을 이용한다. 본 발명에서 예를 들면, patient(1,3), patient(1,7)일 때, 어떤 노드의 레이블의 preorder가 7보다 작으면 patient(1,7)에 있는 노드는 제외하고 사용자 권한을 줄 수 있기 때문에, 더 빠른 접근 제어 방법을 제공할 수 있다.
- <36> 도 3에 도 1에 제시된 트리 구조에 검색 인덱스가 부여된 트리 구조가 제시되어 있다.
- <37> (Group ID, Preorder)에서 Preorder는 전위 순회법에 의한 노드의 방문 순서를 나타낸 것이다. 예를 들어 treatment 노드의 경우에는 보안 레벨이 3이므로 이의 그룹 ID는 3, Preorder는 6 또는 10이므로, 검색 인덱스는 (3,6) 또는 (3,10)이 된다.
- <38> 각 노드에 검색 인덱스가 부여되면 인덱스 부여부(12)는 검색 테이블을 구축하는데, 그 테이블의 일례가 도 4에 제시되어 있다. 검색 테이블은 크게 보안 레벨을 기준으로 구축된다. 이는 노드에 대한 검색이 우선적으로 질의

사용자와 노드의 보안 레벨을 기준으로 이루어지기 때문이다.

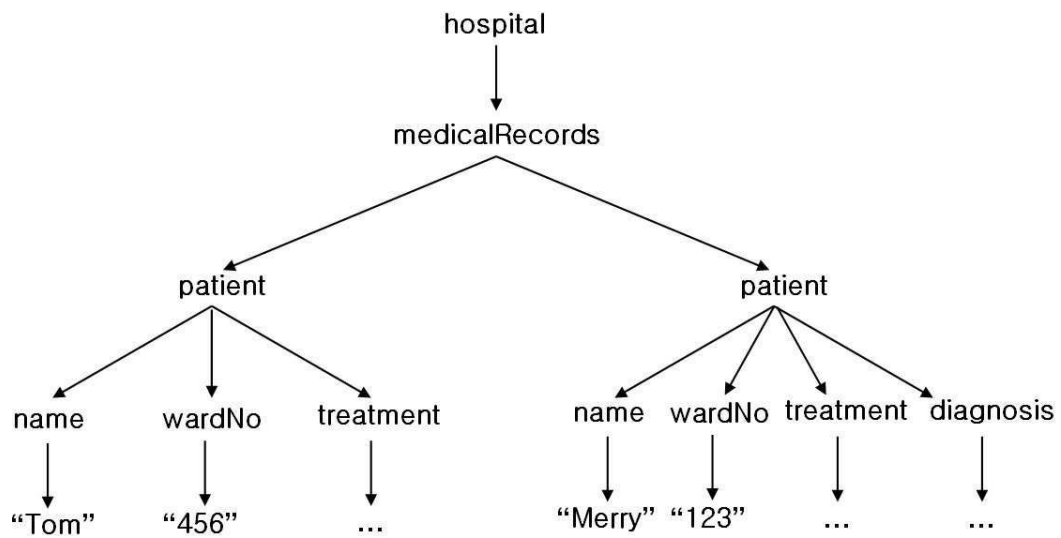
- <39> 사용자로부터 XML 노드에 대한 접근 질의가 들어오면, 노드 검색부(13)는 검색 테이블을 참조하여 검색을 진행하는데, 접근 질의는 XML의 XPath 표현을 이용하여 이루어진다.
- <40> 예를 들어 wardNo 노드에 대한 접근 질의는 {2}://wardNo로 표시할 수 있으며 질의 사용자의 보안 레벨이 2라고 가정하면, 노드 검색부(13)는 이 질의에 대하여 보안 레벨이 1과 2인 검색 테이블만을 참조하여 두 개의 인덱스 (2,5)와 (2,9)를 갖는 wardNo를 검색하여 질의 사용자에게 제공하게 된다.
- <41> 검색(방문) 순서는 위에서 언급한 바와 같이 전위 운행법에 의하여 결정되는 바, 본 예에서는 wardNo 노드에 대한 접근 질의의 경우 인덱스 (1,1)인 hospital 노드, (1,2)인 medicalRecords 노드, (1,3)인 patient 노드, (1,4)인 name 노드, (2,5)인 wardNo 노드, (1,7)인 patient 노드, (1,8)인 name 노드, (2,9)인 wardNo 노드의 순으로 검색을 하여 그 중 접근 질의된 (2,5)인 wardNo 노드와 (2,9)인 wardNo 노드를 질의 사용자에게 제공하게 된다. 보안 레벨이 3인 treatment 노드와 diagnosis 노드에 대해서는 검색조차 이루어지지 아니한다.
- <42> 본 방법발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다.
- <43> 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.
- <44> 이제까지 본 발명에 대하여 그 바람직한 실시예를 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다.
- <45> 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 균등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

도면의 간단한 설명

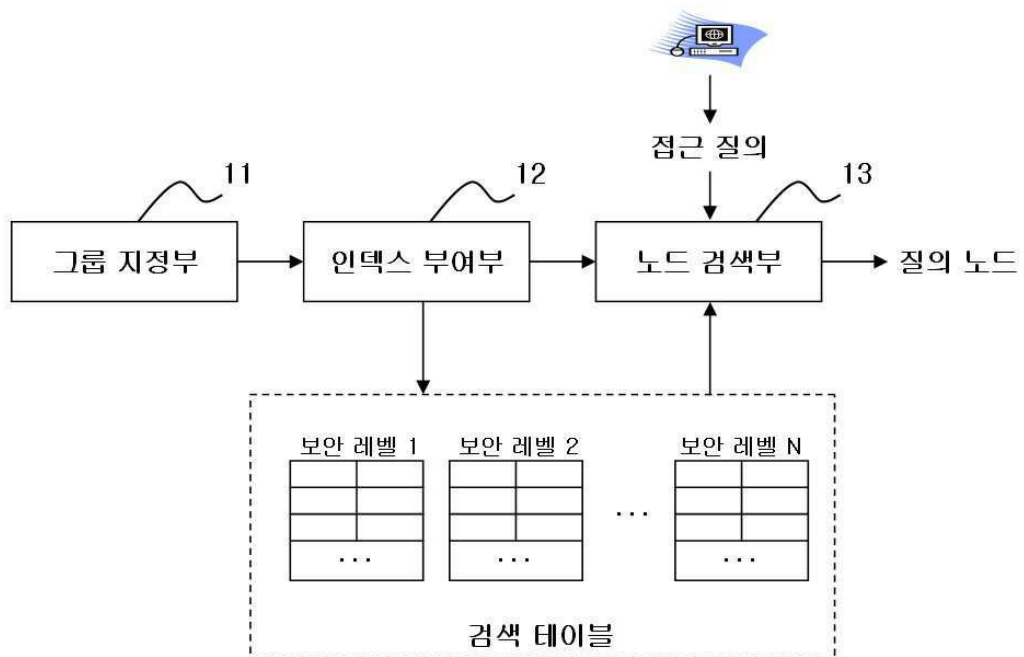
- <46> 도 1은 XML 노드의 구조를 트리(tree) 구조로 표현한 것이다.
- <47> 도 2a는 본 시스템 발명의 바람직한 일실시예의 구성을 나타낸 도면이다.
- <48> 도 2b는 본 방법 발명의 바람직한 일실시예의 흐름을 제시한 도면이다.
- <49> 도 3은 도 1에 제시된 트리 구조에 검색 인덱스(index)가 부여된 트리 구조를 제시한 도면이다.
- <50> 도 4는 노드의 검색에 활용되는 검색 테이블의 일례를 제시한 도면이다.

도면

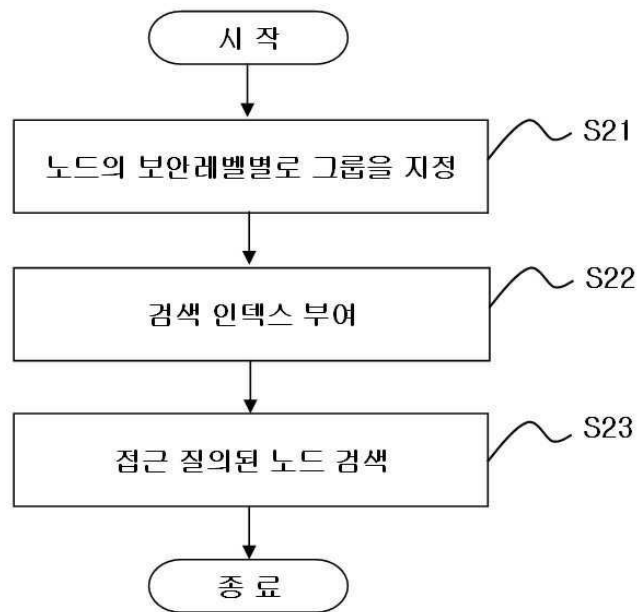
도면1



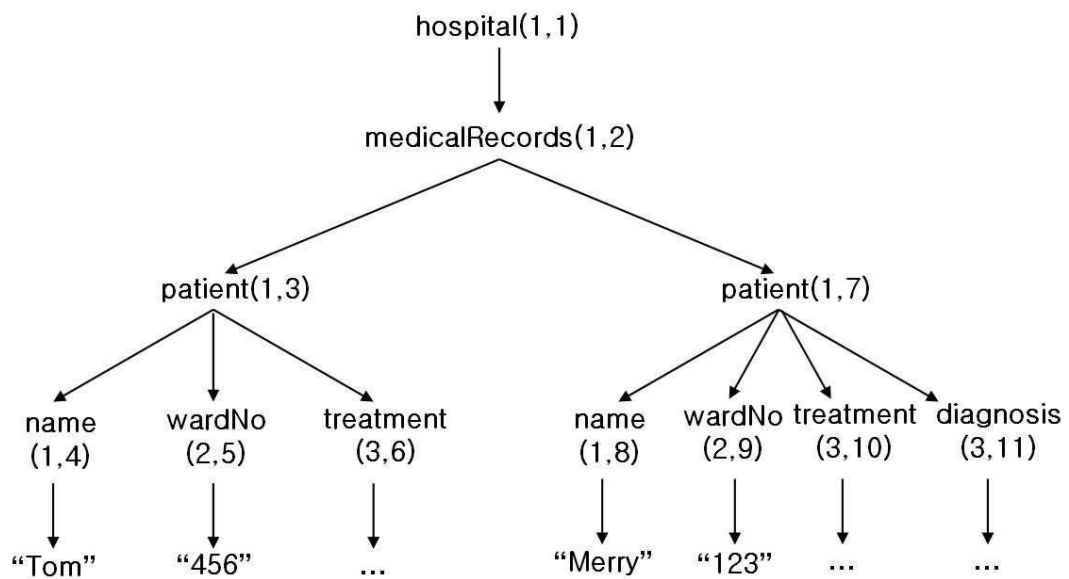
도면2a



도면2b



도면3



도면4

보안 레벨=1		보안 레벨=2		보안 레벨=3	
element	index	element	index	element	index
hospital	(1,1)	wardNo	(2,5),(2,9)	treatment	(3,6),(3,10)
medical Records	(1,2)			diagnosis	(3,11)
patient	(1,3),(1,7)				
name	(1,4),(1,8)				