제22회 한국정보처리학회 추계학술발표대회 논문집 제11권 제2호 (2004. 11)

RFID 태그 시스템을 활용한 문서 유출 방지 및 보안 시스템 연구

윤승배,고혁진,김웅모
성균관대학교 정보통신공학부
Email: spike@ece.skku.ac.kr

A Study of checking a drain of Document and Security System on RFID tag System

Seung-Bae Yun, Hyuk-Jin Ko, Ung-Mo Kim
SungKyunKwan University

요 약

데이터베이스접근기술은 시스템의 보안 모델로서 뿐만 아니라 DRM 기술 및 전자 도서관 서비스등과 함께 활용되어 많은 서비스를 제공하고 있다. 하지만, 시스템 내부의 데이터 보안뿐만 아니라 우리 실생활에서 축척되거나 활용되는 데이터의 보안 또한 매우 중요하다.RFID 태그를 부착한 문서의 정보를 통해 문서 유출을 탐지하고 해당 문서의 정보를 저장하고 있는 시스템의 사용자 접근권한의 변경 및 시스템 내의 보안 정책의 변경을 통해 재차 발생할 수 있는 데이터의 유출을 막도록 하여 시스템 내부의 데이터베이스의 비밀성 및 무결성을 강화할 수 있다.

1. 서론

오늘날 컴퓨터 네트워크 기술의 급속한 발전은 네트워크를 이용한 서비스 다양화를 초래하였다. 그 결과 다방면에 걸쳐 많은 정보를 생산하게 되었고, 이렇게 증가하는 정보를 효율적으로 관리하기 위해 데이터베이스의 유지 및 관리는 필연적이라 할 수 있겠다.

점점 더 거대해져만 가는 대용량의 데이터에 접근하여 해당 서비스를 이용하는 사용자 및 사용자의 요구 사항이 다양해짐에 따라 데이터베이스 보안에 대한 중요성도 나날이 커져만 가고 있다.

그동안 많은 데이터베이스 보안 모델들이 연구되어져 오고 있으며 사용자의 요구 사항의 많은 부분을 충족시켜 나가고 있는 것이 사실이다.

하지만 우리가 그동안 연구해왔던 보안 모델들은 시스템 내부에서의 보안을 위한 데이터베이스 내에서의 사용자 접근을 제어함으로 해당 데이터 객체의 비밀성과 무결성을 보호하는데 주목적이 있었다. 그나마 DRM 기술이나 전자도서관 등의 분야와 접목되어 데이터베이스 접근 기술이 실세계에서 많이 확산되어있지만, 이것조차 데이터가 문서화 되어 우리 조직 내에 어떤 곳으로 이동하여 원래의 목적했던 용도가 아닌 잘못된 곳에 이용되는 것을 탐지 할 수 없고, 재차 발생할 이러한 일들을 막을 수조차 없다. 이러한 데이터의 오용을 막기 위한 RFID태그 기반의 문서 보안 시스템을 제안하려 한다.

본 논문은 2장에서는 그동안 논의 되어왔던 보안 모델들중 RBAC모델 및 디지털저작권보호기술인 DRM과 전자도서관, RFID 태그 기술에 대해서설명하고 3장에서는 보안모델과 RFID 태그를 접목한 시스템을 구축하기 위한 보안 정책 및 시스템을 제안한다. 4장에서는 결론과 향후 연구 방향을 제시한다.

2. 관련 연구

2.1 DRM기술

저작권 관리기술(DRM)은 디지털 컨텐츠에 대한 여러 가지 권리(저작권, 사용권)들을 보호, 관리하는 기술로서 컨텐츠가 네트워크 상에서 전송할 때 이를

보호하기 위한 보안, 불법변조를 방지하기 위한 기술과 방법들, 프로토콜, 알고리즘, 파일형식, 그 밖에 기술들을 의미한다.[1]

2.2 전자도서관

디지털 도서관(Digital Library) 디지털화 된 형태로 구축된 자료를 이용자가 네트워크를 통하여 언제 어디서나 쉽게 접근할 수 있도록 지원하는 시스템이다. 기존의 전통적인 도서관의 확장된 개념으로 정의 될 수 있으며, 사용자의 정보를 제공하는 다양한 정보서비스 시스템까지 포함하는 포괄적인 개념이다.[2]

2.3 RFID 태그 기술

RFID는 라디오 주파수(Radio Frequency)를 이용하며 RFID 시스템은 리더기(혹은 판독기,Reader or Interrogator), 일반적으로 태그(Tag)라고 불리는 트랜스폰더, 컴퓨터 혹은 기타 데이터를 가공할 수 있는 장비로의 세 가지 구성요소가 조합되어 기능을 발휘하도록 구성되어 있다. [3]

태그는 다양한 모양이 가능하며 철제, 목제 문안에 내장할 수 있고 전철이나 버스처럼 외장에 만들 수도 있다. 크기가 다양하며 소형화추세에 따라 플라스틱 카드의 내부나 사람의 피부조직에도 삽입이 가능하며 각종 제품에 내장시키기가 용이하다.

RFID의 작동 원리는 태그가 고유한 정보를 담은 신호를 발생하고 이 신호를 안테나를 통해 콘트롤러가 인식하고 분석하여 태그의 정보를 얻는 방식이다. RFID는 가상세계와 현실세계를 연결하는 링크로서 유비쿼터스 컴퓨팅에 필수적인 요소기술로 모든 상품에 무선 태그를 부착살 수 있다면 다양한 용도로의 활용이 가능해지는데 모든 사물에 RFID를 부착하자는 시도로서 미국 MIT의 Auto ID센터가 대표적이라 할 수 있다.[4]

2.4 RBAC 접근제어 모델

RBAC은 역할에 기반을 두고 사용자의 시스템 자원에 대한 접근을 제어하는 기법이다.[5,6] RBAC 모델의 가장 큰 특징은 권한을 부여하는 단위가 사용자 대신 사용자가 수행하는 기능에 따라 분류에 역할이라는 점이다. 따라서, 사용자는 보호 대상 정보나 자원에 대한 접근 권한을 얻기 위해서는 해당 접근 권한이 배정된 역할의 구성원이 되어야한다. 권한 부여 및 관리 단위가 사용자가 아닌 역할이라는 이 특성은 많은 사용자로 구성된 시스템의 효율적인 권한 관리를 가능하게 한다. 또한 역할간 계층구조를 통해 하위의 역할에 배정된 권한이 상위 역할에 의해 사용될 수 있는 권한 상속(permission inheritance) 특징을 제공한다. 권한 상속 특성을 이용하여 계층구조를 가진 역할들에 대한 권한부여를 효과적으로 실행할 수 있다. 그림 은 RBAC의 기본 모델을 보여주며, 사용자(U:User), 역할(R:Role), 권한(P:Permission), 세션(S:Session)으로 구성되어있다.

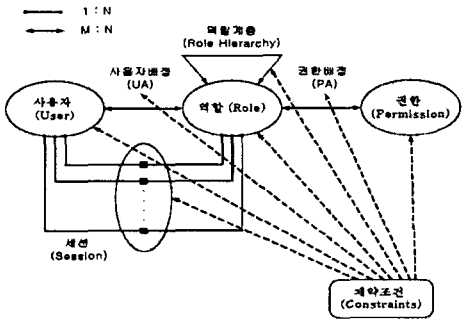
User(U):시스템을 통하여 시스템내의 정보를 사용하는 객체로서 한 사용자는 한명의 사람에 대응된다.

Role(R):접근제어 정책을 구현하는 중요한 의미적구조로서, 조직 내의 직급을 나타내며 고유의 권한과 의무를 갖는다.

Permission(P): 시스템의 하나 또는 그 이상의 객체에 대한 특정 접근 모드(읽기, 쓰기, 수정 등)의 승인을 나타낸다.

Session(S): 시스템의 로그인을 통해 사용자가 수행하기 위한 작업에 대한 역할을 활성화 시킨 상태. 이때 각 세션은 하나의 사용자와 여러 개의 권한을 매칭 한다.

User Assignment(UA) & Permission Assignment(PA): 사용자 배정과 권한 배정은 다대다의 관계이며, 사용자가 정보 객체들에 대해 실행할 수 있는 연산들을 직접 사용자에게 부여하는 대신 역할로 배정하고(PA), 사용자는 해당 역할의 구성원이 됨으로써(UA) 정보 객체에 대한 연산을 수행한다.



[그림 1. RBAC 접근 제어 모델]

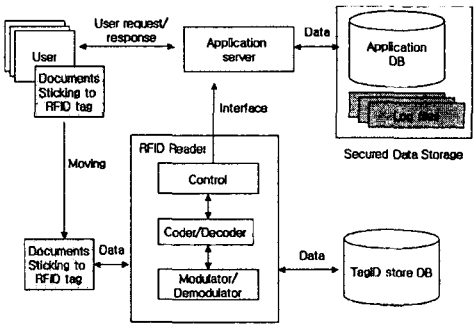
3. RFID 태그를 사용한 문서 유출 방지 및 보안 시스템

[전제조건1]
RFID 태그 부착 문서는 그 위치를 적절히 리더기를 통해 알려주어야 한다.
RFID 태그가 부착된 문서가 위치한 곳에 리더기의 탐색범위가 위치 할 경우 해당 문서의 위치를 탐색할 수 없는 경우가 발생할 수 있다.
[전제 조건2]
RFID 태그가 부착된 문서의 위치 중복을 통한 판독기 충돌은 배재 되어야 한다.
RFID 태그가 부착된 문서의 위치가 다수의 판독기 범위 안에 위치하게 될 경우 해당 문서는 위치가 잘못 인식 될 수 있다.

[정책1]
탐지된 객체의 유효 시간이 정해진 객체의 유효 시간을 넘었을 경우 유출로 본다.
데이터 중 특정 기간 동안 외부로 유출 되거나 일정한 사용자만이 열람할 수 있도록 제약하는 데이터가 여기에 속하는 데이터다.

[정책2]
탐지된 객체의 위치가 정해진 객체의 유효 위치를 넘었을 경우 유출로 본다.
데이터 중 특정 위치에 비치하여 외부인 이나 해당 데이터에 관련이 없는 사용자의 접근을 막기 위해서 데이터의 위치를 제약해야 한다.

본 제안은 특정 데이터 객체에 대한 접근 권한을 소유한 사용자에 의해 특정 데이터 객체가 문서화 하여 사용하는 용도에서 생기게 되는 보안 문제를 다루고 있다. 각 사용자는 시스템 보안 모델에 따라 해당 하는 역할을 할당 받게 된다. 따라서 사용자 및 역할 그룹은 각 객체에 접근이 가능하게 되고, 읽기(Read)나 쓰기(Write) 권한을 소유한 사용자는 각 객체에 원하는 질의를 행사 할 수 있게 된다.
하지만 앞에서 말한 바와 같이 시스템 내에서 보안 문제 뿐만 아니라 해당 데이터를 문서화하여 실생활에 사용할 때도 데이터의 보안 문제가 발생할 수 있게 된다.
현재 사용되는 문서는 시스템의 응용 프로그램에서만이 제어가 가능하다. 가장 일반적인 시스템이 DRM기술을 적용한 논문탐색 싸이트와 전자 도서관 시스템을 예를 들 수 있겠다.
하지만 위의 시스템은 문서화를 막을 수는 있지만, 데이터의 문서화 이후의 오용이나 유출을 탐지 및 추적하기 힘들다.
따라서 특정 등급 이상의 데이터를 문서화 할 경우 해당 문서에 RFID 태그를 부착할 것을 제안한다.
제안 하는 시스템의 구조는 [그림2]와 같다.



[그림 2. RFID tag 기반 보안 시스템 구조]

RFID 태그는 앞에 관련 연구에서 언급한 것과 같이 소형화, 경량화 되는 추세이므로 문서에 RFID 태그를 부착하는 것은 현실적으로 가능할 것으로 본다.
이렇게 문서에 태그를 부착함으로 해서 해당 문서의 위치 및 유출 경로를 추적하여 데이터의 외부로 유출 되는 것을 막을 수 있다.
이때 앞에서 말한 특정 등급의 데이터는 보통의 데이터와 달리 유효 시간과 위치를 제안 하는 속성을 추가적으로 갖게 되고 이는 앞에서 언급한 정책 1(유효 기간)과 정책2(유효 거리)를 반영하기 위한 것이다.
태그가 부착된 문서는 판독기(리더기)를 통해 일정 시간 마다 정보를 back end database에 정보를 전송하게 된다.
문서의 태그 ID는 서버의 요청 시 로그파일로 전송되어 해당 객체와 태그 부착 문서의 일치 여부를 확인하며 이를 통해 해당 객체의 문서화여부를 확인할 수 있고, 문서의 위치정보를 통해 문서가 유효거리 내에 위치한 경우를 탐색해 정해진 위치에서 벗어났을 경우 문서의 유출 여부를 확인 할 수 있다.
제안한 시스템에서 특정 등급의 객체에 대한 정보를 접근한 역할 그룹, 사용자의 ID, 태그 ID와 함께 로그 파일에 저장하게 된다.
사용자 ID 및 데이터 객체 정보를 통해 데이터의 재차 발생 가능한 정보의 남용 및 유출을 막는다.

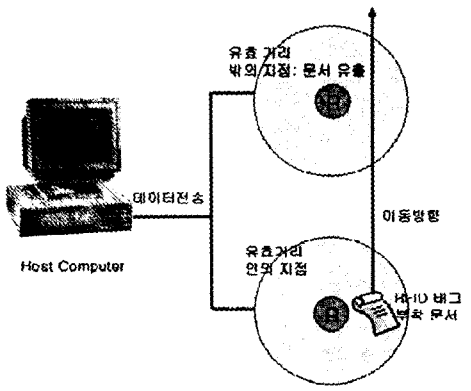
이를 위한 절차 및 정책은 다음과 같다.

첫째, 서버의 로그파일과 전송 받은 태그 ID를 비교해 유출된 문서와 데이터의 일치 여부를 확인한다.

둘째, 일치 여부가 확인 되면 데이터를 접근한 역할 그룹을 탐색한다.

셋째, 유출된 데이터에 접근한 역할 그룹 중 사용자 ID를 찾아 그 사용자의 권한을 조정하여 유출된 데이터에 대한 재차 접근을 막도록 한다.

이때, 또 다른 방법으로 유출의 심각성에 따라 역할 그룹 전체의 접근을 막는 방법을 적용 할 수도 있으며, 해당 데이터 객체의 보안 등급을 상향 조정하여 유출이 발생한 접근 권한 보다 높은 권한을 갖는 역할 사용자들만이 유출된 데이터에 접근하도록 하여 데이터의 비밀성 및 무결성을 보장 할 수도 있다.



[그림 3. RFID 태그 부착 문서의 유출 예]

4. 결론 및 향후 연구 과제

본 논문은 RBAC 데이터시스템을 구축한 환경에서 데이터의 외부 유출을 막고 재차 시도되어질 침입 및 데이터의 유출을 막기 위한 시스템을 제안 하였다.

유비쿼터스 컴퓨팅의 필수 요소를 생각되어지고 있는 RFID 태그는 현재 여러 분야에 응용되어지고 있다. 하지만 앞에 전제조건으로 언급한 바와 같이 태그를 부착한 사물의 위치정보가 정확하게 파악되어야 태그 부착의 주 목적인 문서의 유출 여부를 탐색할 수 있다.

이를 위해서는 RFID 태그내의 데이터와 판독기(리더기)로 정확한 정보를 저장 및 전송 하기 위해서는 RFID 태그 내의 데이터 보안 또한 중요하고, 태그와 판독기(리더기)의 데이터 전송을 위한 네트워크 보안도 이루어 져야 정확한 데이터의 전송이 이루어질 것이다.

그리고 제안 했던 정책을 좀더 구체화 한 접근제어 보완 모델의 연구가 함께 행해져야 할 것이다.

5. 참고 문헌

[1] Carl Gunter, Stephen Weeks, Andrew Wright. "Models and Languages for Digital Rights ", HICSS, 2001

[2] Marko Balabanovic, Yoav Shoham, "Learning Information Retrieval Agents: Experiments with Automated Web Browsing", Proceedings of the AAAI Spring Symposium on Information Gathering from Heterogenous, Distributed Resources, 1995

[3] S.E.Sarma, S.A.Weis, D.W.Engels."RFID Systems and Security and Privacy Implications", Springer-Verlag, 2002

[4] MIT AutoID center Web page, " http://www.autoidcenter.org"

[5] R.Sandhu, E.Coyne, H.Feinstein, and C.Youman, "Role-based access control models", IEEE Computer, Vol. 29,Issue2, 1996

[6] D. Ferraiolo, R.Sandhu, S.Gavrila, D. Kuhn and R.Chandramouli, "Proposed NIST Standard for Role-Based Access Control", ACM Transactions on Information and Systems Security, Vol.4, No3, pp.224-274, Aug.2001