관계형 DBMS에서 목적기반 접근제어 설계

이원철, 이상민

강원대학교 컴퓨터과학과

e-mail:{woncheol, smrhee}@kangwon.ac.kr

Design of Purpose-based access control in Relational DBMS

Won-Cheol Lee, Sang-Min Lee

Dept. of Computer Science, Kangwon National University

요 약

급속한 정보기술의 발달은 기업의 개인 정보 수집, 이용, 제공을 편리하게 만들었으나, 개인정보침해라는 새로운 문제를 발생시켰다. 이러한 문제의 해결을 위해 개인정보 보호를 위한 다양한 연구가 진행되었고, 관계형 DBMS에서 정보의 제공자가 동의한 목적에만 데이터를 사용하는 목적기반 접근제어 모델(Purpose-based access control)이 연구되었다. 목적기반 접근제어를 자동화하기 위해 별도의 메타 DB를 구축하여 사용 목적 준수 여부를 점검하는 방법으로 선 필터 및 질의변환을 사용하였다. 이러한 방법은 신규시스템 구축 시 적용 가능하지만 현재 운영중인 정보시스템 적용에는 한계가 있다. 본 논문에서는 현재 운영 중인 시스템에 적용 가능한 목적기반 접근제어를 데이터 모델과 함수로 설계하였다.

1. 서 론

정보통신의 발달은 기업이 다양한 개인 정보의 수집, 이용, 제공을 가능하게 만들었고, 기업들은 수집된 개인정보를 개인정보 동의 없이 마케팅 및 불법적으로 사용하여 다양한 개인정보 침해사고가 발생하게 되었다. 이러한 문제 해결을 위해 기업의 개인정보 관리 및 보호가 매우 중요한 이슈가 되었다.

정부에서는 개인정보 보호법을 제정하여 정보주체인 개인이 자신에 관한 정보 수집, 이용, 공개, 제공 등을 본인이 통제할 수 있는 권리를 보장하였고, 주민번호와 같은 고유식별정보의 사용을 제한하였으며, 민감정보, 인증정보 등은 관련 법령에 따라 사용을 엄격하게 제한하도록 하였다[1].

기업은 이러한 법령을 준수하기 위해 기존 운영 시스템의 업그레이드 및 개발에 있어 개인정보 보호 및 프라이버시 기술을 고려해야만 한다.

개인정보보호 기술은 두 가지 영역으로 발달하였다. 첫째, 암호화, 침입차단, 디지털 권한 관리 등의 프라이버시 보존 기술이고, 둘째, DBMS에서 통합적인 프라이버시 지원을 위한 방법이 연구되었다. DBMS에서의 프라이버시 지원방법은 역할기반(Role-based) 접근제어 방법에 개인정보의 사용 목적에 따른 접근제어를 접목한 목적기반 접근제어 방법이 주로 연구되었다.

목적기반 접근제어 방법은 개인정보에 대한 사용 목적을 계층화하고, 목적(Purpose)과 의도된 목적(Intended Purpose), 의도된 목적과 저장된 데이터의 연관관계를 정의하여 의도된 목적에 적합한 데이터만 질의처리 가능하도록 설계하였다. 그러나, 시스템 적용에 있어 별도의 질의 변환 및 선 필터를 위해 별도의 메타 DB 및 프레임워크를 구축해야 하기 때문에 기존의 기업 운영시스템에 적용하기 어렵다[2].

본 논문에서는 현재 운영되고 있는 개인정보 수집 동의서의 개인정보처리 동의내역과 역할에 대한 데이터 접근 목적 명세서를 연계하여 개인정보 제공목적과 사용목적이 일치하는 경우에만 데이터를 조회할 수 있는 방안을 제시하였다. 그리고, DBMS에 직접 접근을 하더라도 권한이 없으면 접근을 제한하기 위해 DBMS에서 제공하는 암호알고리즘, 함수와 트리거를 사용하였다.

2. 관련연구

전통적인 DBMS에서의 역할기반 접근제어 방법은 접근제어 관리 작업을 단순화하고 업무에 따른 접근제어 모델을 제공하기 위해, 역할, 사용자, 접근허가 목록, 제약조건을 사용하였고 관리의 효율성을 강화하는 방향으로 연구되었다. ERBAC(Enterprise-Wide Role-Based Access Control) 모델은 역할 할당을 간소화 하기 위해 질의 시 파라미터를 사용하였고[3], GTRBAC(Generalized Temporal Role-based Access Control)는 시간적인 제약사항을 광범위하게 표현할 수 있도록 하였다[4].

PBAC(Purpose Based Access Control)은 저장된 데이터와 의도된 목적을 연결하여 의도된 목적에 맞게 데이터가 사용될 수 있도록 제어하는 방법으로 사용자의 임의적인 데이터 사용을 제한하는 방법이다.

이를 위해 목적을 계층적으로 구성하여 목적트리를 만들고, 데이터와 의도된 목적을 연결한다. 데이터는 테이블(table), 컬럼(attribute), 행(tuple), 이 세가지를 포함할 수 있는 요소(element) 단위로 접근 레벨을 구성한다. 사용자 질의 요청 시 데이터의 제공 목적과 사용 목적의 일치 여부를 검증하는 방법으로 질의 변환을 수행한다[5].

PuRBAC(Purpose and Role-based Access Control)은 목적기반 프라이버시 정책에 기반한 SQL 질의문 수행을 자동적으로 제어하는 시스템적인 접근방법이다. 이를 위해 프라이버시 보장 시스템 개발을 위한 모델기반 개발 프레임워크인 MAPaS(The Modeling and Analysis of Privacy-aware Systems framework)를 구축하고, 데이터 레이어와 PuRBAC 구성을 위한 자바클래스를 생성하여 메타데이터로 구성된 보조 데이터베이스를 구성한다. 프라이버시를 보장하기 위한 질의문 수행을 위해 데이터 사용목적을 점검하여 선 필터처리하고, 세부적인 내용에 대하여 질의문 변환을 수행한다[2].

목적기반 접근제어 방법을 구현하기 위해 별도의 프레임워크 및 메타DB를 구축하는 비용이 발생하고, 시스템 구조를 전체적으로 변경해야 하기 때문에 현재 운영중인 시스템 적용에는 한계가 있다. 그리고 데이터베이스를 애플리케이션이 아닌 직접 접근하는 경우에는 접근제한이 불가능 하다.

3. 제안모델

본 절에서는 목적기반 접근 모델을 지원하는 관계형 ERD를 설계하고, DBMS에서 제공하는 객체만을 사용하여 목적기반 접근모델을 구현하는 방법을 설명한다. 이를 위해, 현재 업무에서 사용되는 개인정보 사용동의 내용과 역할에 따른 사용 목적을 명세화하여 서로간의 일치 여부를 관리하고, 개인정보관리 속성에 대해서는 암호화하여 접근권한이 있는 사람에 한하여 복호화가 가능하도록 구성하여 조회가 가능하도록 한다.

3.1 목적기반 접근제어 모델 설계

관계형 DBMS에서의 목적기반 접근제어 모델 설계를 위해 첫째, 기존의 역할기반 모델에 데이터 사용목적(PurposeOfUse)을 상세화한다. 둘째, 개인정보 제공 동의서 작성시 동의된 개인정보 동의 내역(ListOfConsents)을 항목별로 관리한다. 셋째, 각 개인정보 동의 내역과 관련된 저장 데이터를 관리집합(SetOfManagement)에 저장한다. 넷째, 데이터 사용 목적과 개인정보 동의 내역간의 일치 여부를 관리하는 사용 목적별 개인정보 동의 내역(MappingListOfUseAndConsent)을 정의한다. 다섯째, 고객의 개인정보 동의 내역에 대한 개인별 동의내역(PersonalAgreement)을 저장한다. 그림 1은 관계형 DBMS에서 목적기반 접근제어 모델을 설계한 ERD(Entity Relation Diagram)이다.

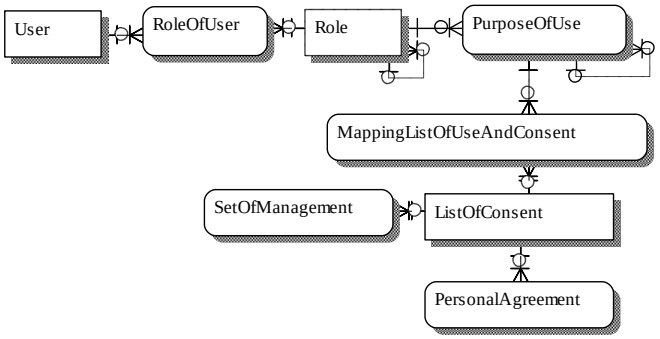

그림 1 목적기반 접근제어 모델 ERD

- **PurposeOfUse**: 업무별 역할에 대하여 데이터 접근 목적을 명세화한 것이다. 예를 들어, 마케팅 담당자의 역할에 데이터 사용 목적은 신규제품의 안내, 계약갱신으로 고객의 이메일, 주소, 전화번호 사용으로 정의한다.
- **ListOfConsent**: 개인정보 수집 시 개인정보 처리(수집, 이용, 제공, 위탁 등)에 동의 내용을 명세화한 것이다. 예를 들어, 신규제품 안내 서비스를 위해 메일, 주소 전화번호 사용을 동의한 내역이다.
- **SetOfManagement**: 개인정보 동의항목에 대하여 포함된 데이터 범위로 속성의 집합으로 구성되어 있다. 예를 들어, 신규제품 안내 서비스를 위해 메일, 주소, 전화번호 사용을 동의하였을 경우, 고객 테이블에 있는 이메일, 주소, 전화번호 컬럼을 관리 대상으로 한다.
- **MappingListOfUseAndConsent**: 사용목적과 개인정보 동의내역이 일치하는 항목에 대한 연관관계를 관리한다. 예를 들어, 마케팅 담당자의 신제품 안내와 개인정보 동의 내역의 동의항목과 일치할 경우 매핑관계를 저장한다.
- **PersonalAgreement**: 개인정보 동의항목에 개인별로 동의한 내역을 관리한다.

3.2 개인정보 관리대상 데이터 암호화

개인정보 관리대상 데이터는 개인정보보호를 위해 암호화하여 저장한다. 암호화된 데이터는 조회 시 암호화된 결과로 조회되어 비 동의된 데이터에 접근하더라도 데이터 값을 식별할 수 없다. 데이터 제공 목적과 사용 목적이 일치하고, 사용자에게 권한이 부여된 역할에 대해서는 복호화가 되어 조회 가능하도록 설계하였다.

그림 2는 **Customer** 테이블로 **email, phone_no, address**가 암호화된 예제이다.

id	name	email	phone_no	Address
0001	John	C82EC65E.	55D052A266E..	CFCC5B8A3….
0002	Bob	C2E881BA.	415B2461AAC..	229B29A155….

그림 2 customer 테이블

암호화 함수는 복호화가 가능한 함수를 사용하며 Trigger에 적용하여 데이터 입력, 수정, 삭제 시 별도의 추가적인 작업이 필요 없도록 설계한다. 그림 3은

Customer 테이블 데이터 저장 시 암호화 **trigger** 예제이다.

```
Create Trigger encrypt_customer on customer
Begin
  If inserting or updating or deleting then
    new.email := encrypt(email);
    new.phone_no := encrypt(phone_no);
    new.address := encrypt(address);
  end;
End;
```

그림 3 암호화Trigger 예제

3.3 개인정보 관리대상 데이터 조회 함수

암호화된 관리대상 데이터는 조회 함수로만 접근이 가능하다. 조회 시 사용자 아이디와 컬럼명을 매개변수로 사용한다. 그럼 4는 관리대상 조회 알고리즘이다. 먼저, 사용자에 대한 역할을 조회한다. 둘째, 역할에 대한 접근사용 목적 리스트를 조회한다. 셋째, 목적 리스트에 대한 동의 항목을 조회한다. 넷째, 동의 항목에 대한 컬럼을 조회한다. 다섯째, 동의 항목에 대한 개인 동의 여부를 조회한다. 마지막으로, 개인이 동의하였다면 복호화 함수를 통해 데이터를 조회하도록 한다.

```
Algorithm read_column(User_Id, Column_Name)
1: search Role_Id from RoleOfUser where user_id = User_Id
2: search AccessPurpose_Id from PurposeOfUse
   where role_id = Role_Id
3: searach Agreement_List from MappingListOfUseAndConsent
   where accesspurpose_id = AccessPurpose_Id
4: search column_list from SetOfManagement
   Where list_consent = List_Consent
5: search Personal_agreement from PersonalAgreement
    where list_consent = List_Consent
6: if personal_agreement is true then decrypt(column) else null
```

그림 4 관리대상 조회 함수 알고리즘

3.4. 질의문

본 논문에서 제안된 방법은 정보제공자가 사용목적에 동의한 내역과 접근 사용 목적에 일치하는 경우에만 데이터가 조회될 수 있도록 구성하기 위해 별도로 작성된 조회 함수를 질의문 작성시 사용한다. 질의문 작성시 관리 대상이 되는 컬럼에 대하여 사용자 아이디와 관리항목 컬럼을 매개변수로 사용한다.

그림 5는 마케팅 담당자가 신규상품 안내를 위해 고객들에 대한 정보를 조회하는 질의문 예제이다.

```
Select id, name,
      read_colum('marketer',email, user_id),
      read_colum('marketer',phone_no, user_id),
      read_colum('marketer',address, user_id) from customer
```

그림 5 질의문 작성 예

그림 6은 질의에 대한 결과로 정보 제공자가 동의한 내역만 결과로 조회가 되는 예제이다.

id	name	Email	phone_no	Address
0001	John	john@sn.com	010-0010-0001	seoul
0002	Bob	null	null	null

그림 6 질의 결과

4. 결론

본 논문에서는 현재 운영되고 있는 관계형 DBMS에 적용 가능한 목적기반 접근제어 모델을 설계 및 구현하였다. 이를 위해 역할에 개인정보 사용 목적을 명세화 하였고, 개인정보 수집 시 개인정보 처리 동의 내역을 명세화하여 일치하는 항목에 대하여 매핑관계를 관리하도록 하였다. 또한 데이터 접근 시 접근 동의된 항목에 대해서만 조회 가능하도록 관리대상이 되는 항목을 암호화하여 접근권한이 없는 사용자의 접근을 DBMS에서 제한하였다.

본 논문은 목적기반 접근제어 모델을 관계형 DBMS에 적용 할 수 있도록 설계하여 별도의 프레임워크 및 메타DB 구축 없이 기업시스템에 적용할 수 있는 우수한 결과로 사료된다.

참고논문

[1] https://www.privacy.go.kr/

[2] P. Colombo, E. Ferrari "Enforcement of Purpose Based Access Control within Relational Database Management Systems," IEEE Transactions on Knowledge and Data Engineering, Vol.26, pp.2703-2716, Nov. 2014.

[3] A., Kern, "Advanced Features for Enterprise-Wide Role-Based Access Control," Proc. of Annual Computer Security Applications Conference, Las Vegas, Nevaea, pp. 333-342, 2002,

[4] J., b. d. Johsi, E., Bertino, U., Latif, and A., Ghafoor, "A Generalized Temporal Role-Based Access Control Model," IEEE Transactions on Knowledge and Data Engineering, vol.17, pp. 4-23, 2005

[5] J. B. Byun., N. Li, "Purpose Based Access Control for Privacy Protection in Relational Database System." The VLDB Journal, vol.17, no.4, pp.603-619, 2008.