전자상거래에서 가변적 개인정보 동기화 통합 관리모델 설계

한정호*, 이영진*, 이상호*
충북대학교 전자계산학과 네트워크 & 보안 연구실
e-mail : right@netsec.chungbuk.ac.kr

The design of Variable Privacy Synchronization Unification Model on EC

Jeong-Ho Han*, Young-Jin Lee*, Sang-Ho Lee*
Dept of Computer Science, Chung-Buk University

요 약

최근 첨단 정보기술의 발전과 함께 지식정보사회로 진환되면서 전자상거래 분야가 빠르게 성장하고 있다. 전자상거래는 거래를 통해서 많은 개인정보를 수집, 관리 및 생성하게 되는데 일단 수집된 개인정보는 개인정보 주체의 꾸준한 갱신이 없다면 개인정보에 대한 기본 요구사항이자 개인정보 보호법에서 개인정보 주체의 의무사항인 최신성과 정확성이 결여된 상태가 된다. 따라서 이 논문에서는 최신성과 정확성의 결여로 발생되는 정확한 서비스와 사용목적 및 용도 변경시 동의를 받을 수 없는 문제, 수집된 개인정보를 주체는 어느 사이트에서 사용되고 있는지 알지 못하는 문제를 해결하기 위해 전자상거래에 사용되는 개인정보를 가변적 개인정보와 불변적 개인정보로 분류하고, 이를 기반으로 각 전자상거래 사이트들이 수집한 가변적 개인정보를 통합적으로 관리해 주는 방식의 최신성과 정확성을 충족시킬수 있는 통합 모델(Privacy Synchronization Unification Model)을 제안한다.

1.서론

인터넷의 사용이 급증하고 B2B, B2C 등 전자상거래가 활성함에 따라 개인정보의 유통은 피할 수 없는 대세가 되고 있다. 많은 전자상거래 사이트들은 개인정보를 수집하게 되었고, 개인정보의 주체들은 수 많은 사이트들에 자신의 개인정보의 수집을 허락하였다. 하지만 자신의 개인정보가 수집된 전자상거래 사이트들을 일일이 기억할 수 없다. 개인정보 주체의 변경된 개인정보가 수정되지 않음으로 인해 사용자들은 양질의 서비스와 사용목적 및 용도 변경시 동의를 받을 수 없으며, 또 개인정보보호법에서 제시한 정확성의 원칙을 지킬수가 없다. 또한 불필요한 전자상거래 사이트의 개인정보 삭제하기가 불가능한 실정이다.

이 논문에서는 개인정보의 기본 요구사항이며, 개인정보보호법에서 제시한 개인정보 주체의 의무인 정확성 및 최신성을 유지하기 위해 개인정보를 가변적·불변적으로 구분하고, 가변적 개인정보 통합 관리모델 PSUM(Privacy Synchronization Unification Model)과 알고리즘을 설계하여 문제점의 해결 가능함을 보인다.

이 논문의 구성은 다음과 같다. 2절에서는 개인정보 동기화를 위한 관련연구를 기술하고 3절에서는 전자상거래에서의 가변적 개인정보를 분류하고, 가변적 개인정보 동기화 통합 모델을 설계 및 알고리즘을 제시한다. 4절에서는 PSUM에 대한 평가를 하며 마지막으로 5절에서는 결론 및 향후 연구과제를 기술한다.

2. 관련 연구

개인정보는 생존하고 있는 개인에 관한 정보로서 성명·주민등록번호등에 의하여 당해 개인을 식별할 수 있는 부호·문자·음성·영상 및 생체 특성등에 관한 정보를 말한다[1].

2.1 프라이버시 조약

① 개인정보 보호 지침

개인의 사생활의 비밀을 보호하고 사적 권익의 침해를 방지하기 위하여 제정된 지침이고, 제 9조에 정확성을 유지해야 할 의무를 명시하고 있다[1].

② OECD 국제 프라이버시 조약

OECD 국제 프라이버시 조약 8원칙(수집 제한의 원칙, 정보의 정확성의 원칙, 목적 명확화 원칙, 이용제한의 원칙, 안전 보호의 원칙, 공개의 원칙, 개인 참여의 원칙, 책임의 원칙:1980)을 제시함으로 국가간 지켜야할 프라이버시 조약을 규정하였다[2].

③ EU 조약

회원국의 개인정보를 제 3국으로 이전하기 위해서는 목적제한, 정보의 질, 투명성, 안전성, 열람·정정·거부, 정보이전의 제한의 원칙을 제시함으로 회원국간에 개인정보 유통시 기준을 마련하였다[3].

2.2 국내 개인정보 보호 마크제도(EPRIVACY)

공신력있는 기관이 인터넷사이트의 개인정보보호 및 내부관리 체계등의 수준등을 전문적으로 평가하여 일정 요건 충족시 마크를 부여하여 인터넷 사이트 개인정보 보호 수준을 인증하는 제도이다.

2.3 P3P(Platform for Privacy Preference)

MS Explorer 6.0에서 일부 적용된 기술로 특정 웹사이트의 프라이버시 정책을 사이트 접속자에게 알려줌으로써 개인이 자신에 대한 정보를 제공할지 여부를 결정할 수 있도록 한다[7].

3. 가변적 개인정보 통합관리 모델

3.1 가변적 개인정보의 정의

가변적 개인정보란 개인을 식별할 수 있는 개인정보(성명·주민등록번호등)중 과거의 일정시점에서는 정확한 것이었다 할더라도 현시점에서 그 사실에 변화가 있을 수 있는 개인정보를 의미한다. 단 이 논문에서 법적 재판을 통해 변경가능한 개인정보 항목은 불변적 개인정보 항목으로 규정짓는다.

3.2 가변적 개인정보의 분류

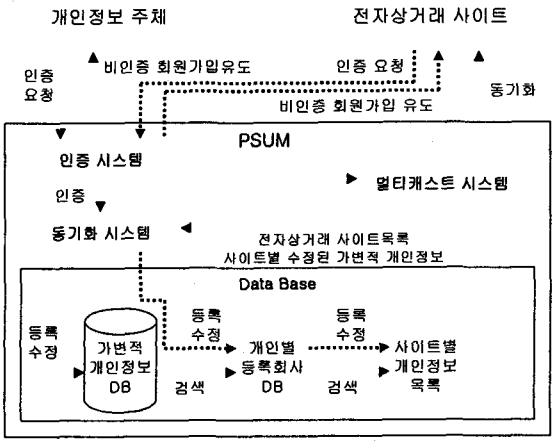
[표1]은 전자상 거래에서 전자상거래 사이트가 일반적으로 수집하는 개인정보 목록을 불변적·가변적으로 구분한 표이다.

전자상 거래 개인정보의 종류	
불변적 개인정보	가변적 개인정보
이름 주민등록번호 생년월일 성별	주소(자택, 직장) 전화번호(자택, 직장) 핸드폰번호 학력 전자우편(e-mail) 혼인여부 선호하는 스포츠 오락 여가활동

[표1] 전자상거래에서의 가변적·불변적 개인정보 분류

3.3 PSUM

다음의 [그림1]은 개인정보 주체나 전자상거래 사이트가 인증되면 동기화 시스템을 통하여 가변적 개인정보와 개인정보 등록 사이트목록 그리고 전자상거래 사이트별로 수집하는 개인정보 목록의 통합관리로 PSUM에서 가변적 개인정보를 개인정보 주체가 변경시 그 주체가 등록해 놓은 사이트를 검색하여 수정된 가변적 개인정보를 해당 전자상거래 사이트에 전송해줌으로 동기화하는 PSUM의 시스템 구성도이다. 이 연구에서 PSUM은 보안상 안전하다고 가정한다.



[그림1] Privacy Synchronization Unification Model

① 인증시스템

개인정보 주체 및 전자상거래 사이트를 인증한다. 비인증시 다시 개인정보 주체 및 전자상거래 사이트들에게 PSUM에 등록을 유도한다. PSUM을 활용하

기 위한 가변적 개인정보 동기화에 대한 개인정보 주체에 대한 동의가 있다고 가정한다.

[표2]는 인증시스템의 주요 알고리즘의 설계이다.

```
- 인증부분 -
select id, id_no from member where id = '& id
'
   If count = 0 then
      회원 가입 유도(PSUM에 등록유도)
      break
   End If
```

[표2] 인증 시스템 알고리즘

② 동기화 시스템

개인의 가변적 개인정보, 개인이 귀속되어 있는 전자상거래 사이트 목록, 각 전자상거래 사이트들이 요구하는 가변적 개인정보 목록과 데이터를 검색 및 관리한다.

개인정보 주체가 동기화 시스템에서 가변적 개인정보를 수정하면, 수정된 가변적 개인정보가 등록되어 있는 회사 DB를 검색한다. 이 부분에서 개인정보 주체는 자신의 개인정보가 등록되어 있는 회사를 검색이 가능하다. 전자상거래 사이트별 개인정보목록을 검색하여 해당 수정된 가변적 개인정보만을 멀티캐스트 시스템으로 보낸다.

전자상거래 사이트의 등록의 경우 전자상거래 사이트별 개인정보 목록에 해당 전자상거래 사이트의 가변적 개인정보를 등록하고 개인별 등록회사에 수집된 개인정보 주체와 가변적개인정보 DB의 주체와 주민등록번호로 일치함을 보이면 등록한다. 이때 개인의 식별자로는 주민등록번호를 사용한다.

[표3]은 동기화 시스템에 대한 주요 알고리즘이다.

```
- 가변적 개인 정보 등록 -
J = 0  '회사 리스트 변수
I = 0  '정보 리스트 변수
가변적 개인 정보 update
insert into 회원 values(항목1, 항목2, 항목3.....)
- 등록된 회사 이름 구하기 -
select 회사테이블에 이름필드 from company
where field(주민번호) = & 회원의 주민 번호
- 등록된 회사의 개인 정보 리스트 구하기 -
do while( 개인별 등록회사 )
   select * from 회사테이블의 이름필드 where
field(아이디) = & id
   do while ( 개인 정보 ) - ·목록 검색
      If 개인정보 목록.이름 = 가변적 개인정보
(수정된 내용) 목록.이름 then
         개인정보 목록(j)(i) = 수정된 개인 정보
      End If
      I = I + 1
      Next
   Loop
   J = J + 1
   Next
Loop
- 전자상거래 회사 등록 -
select 회원테이블의 주민번호필드 from 회원
order by no asc  '회원으로 가입을 원하는 회사의
회원 주민번호를 다 가져온다
Do While ( 회원 )
   select * from 회사 where field(주민번호) =
& id_no
   If count > 0 Then
      insert into 회사 회원테이블 values(번호,
사용자, 사용자 주민번호, 회사 이름, 날짜)
   End If
Loop
- 전자상거래 사이트 개인정보 목록 등록 -
insert into company.name values(개인정보1, 개인
정보2, 개인정보3,.....)
```

[표3] 동기화 시스템 알고리즘

③ 멀티캐스트 시스템

전자상거래 사이트들에게 가변적 개인정보를 전송하는 부분들을 담당한다. 동기화 시스템에서 받은 개인별 전자상거래 사이트 등록 목록과 개인별 수정된 가변적 개인정보를 통해 해당 전자상거래 사이트로 수정된 가변적 개인정보만의 전송한다. 가정으로는 멀티캐스팅시 해당되는 모든 전자상거래 사이트들에게 수정된 가변적 개인정보는 반드시 전송된다.

[표4]는 멀티캐스트 시스템에 대한 주요 알고리즘이다.

```
For J = 0 To Ubound(개인정보 목록( )( ) )
   회사별 개인 정보(j)(i) 전송
Next
```

[표4] 멀티캐스트 시스템 알고리즘

4. 평가

개인정보를 가변적, 불변적으로 구분하여 가변적 개인정보를 통합 관리모델(PSUM)을 통하여 동기화 한다. 가변적 개인정보를 3.3에서 제시한 PSUM과 각 구성요소 인증시스템, 동기화시스템, 멀티케스트 시스템의 알고리즘을 활용하면 다음과 같은 문제점이 해결 가능하다.

첫째 개인정보 보호법, OECD국제 프라이버시 조약, EU 조약, 일본통산성 개인정보 처리지침 등에서 제시하는 개인정보의 최신성, 정확성을 유지하지 못했던 기본적 의무 조건을 만족할 수 있다.

둘째 이 제안모델을 통해 사용자들은 별도의 어려움 없이 모든 개인정보 주체가 개인정보 수집을 동의한 사이트의 개인정보를 검색, 수정 및 삭제의 관리가 가능하다.

셋째 가변적 개인정보의 정확성으로 인해 개인정보 주체는 전자상거래에서 제공하는 서비스를 정확하게 받고, 전자상거래 사이트는 정확한 서비스 할 수 있다.

넷째 가변적 개인정보에 대한 정확성 및 최신성으로 개인정보를 수집한 전자상거래 사이트가 수집한 개인정보에 대한 사용 목적 및 용도 변경시 개인정보 주체의 동의를 정확히 받을 수 있다.

5. 결론 및 향후 연구과제

최근 첨단 정보기술의 발전과 함께 지식정보사회로 전환되면서 전자상거래 분야가 빠르게 성장하고 있다. 전자상거래는 거래를 통해서 많은 개인정보를 수집, 관리 및 생성하게 되는데 일단 수집된 개인정보는 개인정보 주체의 꾸준한 갱신이 없다면 개인정보에 대한 개인정보의 기본 요구사항인 최신성과 정확성이 결여된 상태가 된다.

이 논문은 개인정보 보호법, OECD국제 프라이버시 조약, EU 조약, 일본통산성 개인정보 처리지침등에서 제시하는 기본의무인 최신성과 정확성의 결여로 인해 발생되는 문제를 해결하기 위하여 전자상거래시 요구되는 가변적 개인정보를 동기화하는 모델을 제시하였다. 이 PSUM은 여러 전자상거래 사이트에 수집되어 있는 개인정보를 쉽게 수정, 삭제 및 관리를 할 수 있으며, 개인정보를 수집한 사이트가 개인정보를 다른 용도로 사용시 개인정보 주체에게 동의를 받을 수 있으며, 전자상거래 사이트와 개인정보 주체는 정확한 서비스를 제공하고 제공받을 수 있다. 또한 여러 국제 프라이버시 조약등에서 제시하는 기본 요구사항인 최신성 정확성을 충족함으로 앞으로의 개인정보 보호 및 관리 모델의 필수 구성요소로 활용 가능하다.

향후 연구과제로는 너무 많은 가변적 개인정보를 정보를 한곳 보관 관리하고 있다는 보안적 문제점과 많은 양의 가변적 개인정보 동기화, 관리 및 처리로 발생되는 시스템 부하문제들을 들수 있다.

참고 문헌

1. 한국정보보호진흥원, "개인정보 보호지침", 2002.1.18
2. OECD, "Transborder Data Flow Contracts in the Wider Framework Of Mechanisms for Privacy Protection on Global Network", DSTI/ICCP/REG(99)15/FINAL, Septmber 2000
3. 유럽연합' "EU 조약(국가간 개인정보보호지침)", 1998.10.15
4. 일본통산성, "일본 통산성 개인정보 보호 지침"
5. 한국정보보호 진흥원, "2002 개인정보 백서", 2002
6. 정보보호위원회 사무국 "프라이버시 마크심사기준"
7. http://www.w3.org/P3P
8. 한국교육신문, "NEIS 시행되면 매트릭스에 갇힌 인간 된다?", 2003. 6. 19
9. Jeffrey A Griffin, "Privacy and Security in the Digital age", IEEE, 1998
10. Gunter Karjorth, Matthias Schunter, Michacl Waidner, "Platform for Enterprise Privacy Practices:Privacy-enabled Management of Customer Data". Lecture Notes in Computer Science, Springer Verlag, 2002
11. Frans A. Lategan, Martin S. Olivier, "A Chinese Wall Approach to Privacy Policies for the Web", 26th Annual International Computer Software and Applications Conference August 26 - 29, 2002