u-IT 환경에서의 개인화서비스를 위한 개인정보 보호방안 연구

A Study on a Protection of Personal Data for Personalized Services in Ubiquitous Environment

김영삼 (Y.S. Kim) 인증기술연구팀 UST 연구생
박주영 (J.Y. Park) 인증기술연구팀 인턴연수생
진승헌 (S.H. Jin) 인증기술연구팀 팀장

목 차

인터넷 이용이 활성화되면서 온라인서비스의 종류와 양은 계속 증가하고 있다. 최근에 서비스제공자들은 이러한 다양한 서비스들을 효율적으로 제공하기 위해 개인화서비스를 제공하기 시작하였고, 이에 따라 개인정보의 중요성은 더욱 증대되고 있다. 하지만 개인정보의 수집은 프라이버시 침해 문제를 유발할 수 있어 개인화서비스는 쉽게 적용되지 못하고 있다. 또한, 다가오는 유비쿼터스 환경에서는 수집 가능한 개인정보의 증가가 예상되며, 따라서 프라이버시 침해 문제는 더욱 심각해질 것으로 예상된다. 본 고에서는 개인화서비스 모델에 대해 소개하고, 개인정보 보호를 위한 기존 기술들에 대해 분석하여, 유비쿼터스 환경에서의 개인화서비스를 위한 개인정보 보호방안에 대한 제언을 하고자 한다.

Ⅰ. 서론

과거의 산업사회에서는 TV, 라디오, 신문, 잡지 등의 대중매체를 통해 마케팅을 하는 것이 일반적이었다. 이러한 대중매체들은 시간(광고시간)과 공간(지면)의 제약이 있었고, 서비스제공자들은 사용자들이 원하는 모든 정보를 제공해 줄 수 없었다. 서비스제공자들은 효율적인 마케팅을 위해 다수가 만족할 수 있는 공통적인 관심사에 대해 마케팅을 하게 되었다. 서비스제공자가 모든 고객의 니즈(needs)를 완벽히 만족시킬 수는 없었지만 대부분의 사용자들은 니즈 충족을 위한 비용(원하는 정보를 찾는 것)이 너무나 컸기 때문에 이러한 서비스를 이용할 수 밖에 없었다.

인터넷이 등장하고 소위 정보화가 이루어지면서, 인터넷이 주요 대중매체로 부상하였다. 인터넷의 특성상 시간, 공간의 제약이 없었고 이에 따라 인터넷에는 많은 정보들이 쌓이기 시작했다. 또한 양방향 커뮤니케이션이 가능해짐으로써 고객들은 이제 자신이 원하는 정보를 능동적으로 찾을 수가 있었다. 이에 따라 고객들은 기업이 제공하는 서비스가 정말 자신의 니즈에 맞는 것인지, 더 나은 서비스는 없는 것인지 등에 대해서 스스로 판단하고, 선택할 수 있게 되었다. 기존의 mass marketing은 효율성이 떨어졌다.

한편, 인터넷의 발전은 새로운 문제점을 낳게 되었는데, 그것은 바로 정보의 양이 지나치게 많아졌다는 것이다. 비대해진 인터넷에서 원하는 정보를 찾기 위해 사용자들은 더 많은 시간을 들여야 했다. 서비스제공자의 제한적 정보제공이 문제였던 산업사회의 문제점을 해결해주었던 인터넷이 이제는 너무나 많은 정보의 제공으로 문제가 된 것이다.

이러한 문제점을 해결하기 위해 서비스제공자들은 표적 시장을 점점 소규모화, 세분화하여 사용자들의 개인화된 요구사항을 만족시키고자 하였고, 그 결과 개인화서비스가 등장하게 되었다.

개인화서비스란 고객 개개인의 니즈를 파악하여 그에 맞는 서비스를 하는 것이다. 기업이 고객 개개인의 니즈를 파악하여 서비스를 하기 때문에, 고객들은 원하는 정보를 찾아야 하는 수고를 덜 수 있고, 기업은 적중률 높은 서비스를 제공함으로써 비용효율(cost-efficiency)을 높일 수 있다.

개인화서비스는 새로운 서비스 패러다임으로써 기업의 효율적인 서비스를 가능하게 하지만, 이를 위해서는 고객 개개인의 정보를 수집하고 분석해야 하며, 이는 고객의 프라이버시 문제와 직결된다. 실제로 몇몇 개인화 서비스들은 시행 초기단계에 시민단체의 반발에 부딪쳐 난항을 겪기도 한다(e.g. KT의 스마트웹 서비스). 개인화 서비스가 문제가 되는 부분은 바로 개인정보의 수집 및 이용과정에서의 프라이버시 침해이다.

현재 온라인상에서 이루어지는 개인정보 수집 방법은 사용자의 동의를 통해 이루어지고는 있지만, 이는 매우 낮은 수준의 프라이버시 보호수단이다. 개인정보가 실시간으로 수집되고, 동태적인 정보까지도 수집될 수 있는 유비쿼터스 환경에서 현재의 방법으로는 프라이버시 보호를 기대하기는 더욱 힘들다. 본 고에서는 현재 개인화서비스를 위한 개인정보 수집 및 이용 모델에 대해 조사, 분석하여 장단점을 파악하고, 유비쿼터스 환경에서 프라이버시를 보호할 수 있는 안전한 개인정보 수집 및 이용 모델의 방향을 제시한다. 또한 개인정보 수집 시에 적용되는 프라이버시 보호 기술들에 대해 조사, 분석하여 문제점을 파악하고, 그것을 개선할 수 있는 방안을 제시한다.

Ⅱ. 개인화서비스 모델

개인화서비스란 고객들의 니즈를 예측하고 더욱 효과적인 상호작용을 만듦으로써 웹 상호작용에 부합하는 기술 및 고객정보를 이용하는 것을 말한다[1]. 이러한 개인화서비스를 위한 가장 기본적이면서도 중요한 과제 중 하나는 개인정보의 안전한 수집 및 이용이다.

개인정보를 수집하고 이용하는 모델은 크게 CRM과 VRM 두 가지가 있다. 현재 많이 사용되는 모델

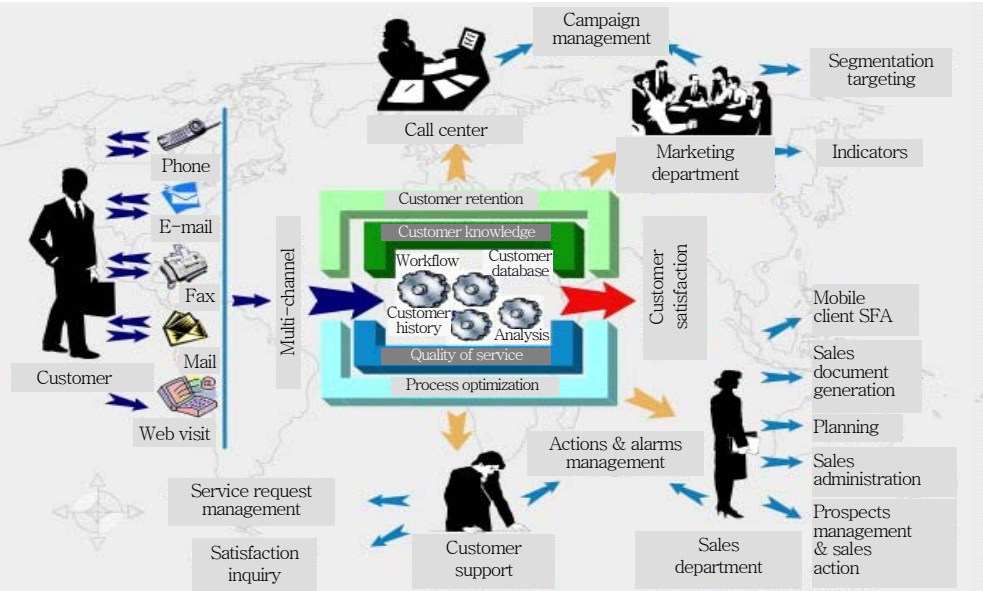
은 CRM이며 이는 기업주도적인 형태를 가진다. VRM은 CRM과 대비되는 개념으로써, 최근에 조명을 받고 있는 모델이다. VRM은 개인정보 관리의 주체가 개인이며, 개인이 중심이 되어 기업(vendor)들을 관리(manage)한다. 본 절에서는 두 가지 개인정보 수집 및 이용 모델에 대해 분석하고 유비쿼터스 환경에서 어떤 모델이 적합한지 알아보도록 한다.

1. CRM

CRM이란 기업이 잘 정리된 방법으로 고객관계를 관리해 나가기 위해 필요한 방법론이나 소프트웨어 등을 말한다[2]. CRM의 주체는 기업, 즉 서비스 제공자가 된다. 개인정보의 수집 주체가 기업이기 때문에 사용자는 비록 형식적인 절차는 거치지만 정보제공에 대해 수동적인 입장이 분명하다. 이는 기업이 개인정보를 보관, 관리하기 때문에 정보의 집중화 문제(big brother)가 발생할 수 있으며, 프라이버시 침해의 소지가 다분하다. 최근의 전자상거래 사이트에 대한 해킹사고를 보면, 개인정보의 유출이 기업에게 어떠한 피해를 입힐 수 있는지 여실히 보여준다. 기업은 이러한 정보 유출을 방지하기 위해 다양한 보안장치를 도입하고 있지만, 유출 사고는 끊임없이 일어나고 있으며 이에 따르는 기업의 소모비용은 적지 않다.

기업이 이러한 프라이버시 침해 및 정보의 집중화, 해킹피해에 대한 잠재적 피해액 증가 등을 감안하면서까지 개인정보를 수집하려 하는 것은 개인정보가 그만한 가치가 충분하기 때문일 것이다. 개인정보를 수집하고 분석하여 새로운 고객을 유치하는데 사용하거나 능동적인 일대일 마케팅을 펼침으로써 고객만족(customer satisfaction)을 실현하고자 함이며, 이는 기업의 이익 증대와 연관성이 있다.

반면, 고객의 입장에서 보면 CRM은 장점보다는 단점이 더 많다. 과거와는 달리 개인정보에 대한 중요성이 부각되고 있는 현실에서, 고객들은 자신의 정보를 개인화서비스라는 명목 하에 기업이 수집하고 이용하는 것에 대해 불안함을 느낄 수 있다. 이러한 불안 요소를 제거하기 위해서 기업들은 서비스 이용을 위한 개인정보의 수집시 사용자의 동의를 얻는 절차를 두고 있다. 이는 개인정보 수집의 목적 및 이용범위 등을 고지하도록 강제하고 있는 개인정보



<자료>: http://www.amigolog.com/ConsultancyCRM.phtml

(그림 1) CRM 개념도

보호법에 근거하는 것이며, 따라서 법적 효력은 확실하다고 할 수 있다. 하지만 기업이 이러한 고지를 하는 시기는 서비스에 가입할 때이다. 서비스에 가입할 때 사용자는 기업이 자신의 정보를 이용하여 어떠한 정보를 만들어 낼 것이고, 그것이 자신에게 얼마만큼의 영향을 줄 것인지를 미리 안다는 것은 어려운 일이다. 이에 현재 개인정보 수집에 동의 후에도 그것을 철회할 수 있는 제도가 필요하며, 현재 일부 도메인에서 관련 법률이 개정된 상태이다[3].

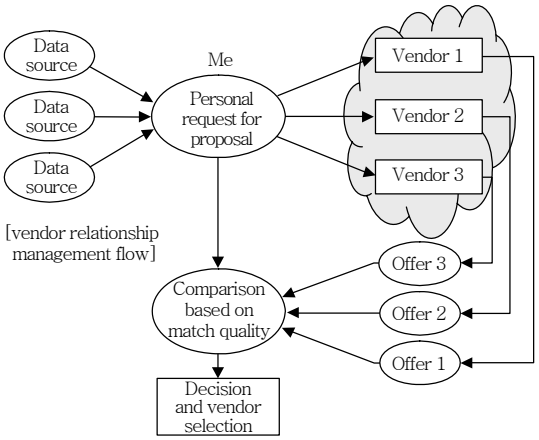
CRM은 기업 중심의(enterprise-centric) 개인정보 수집 모델로서, 개인정보의 보호관점에서는 보완해야 할 점이 많은 것이 사실이다. 하지만 기업의 입장에서는 능동적인 마케팅 및 개인화서비스를 할 수 있는 CRM을 선호하는 것이 사실이며, 이에 대한 문제점들은 앞으로 계속 보완해 나가야 할 것이다((그림 1) 참조).

2. VRM

VRM은 CRM과는 보완 대체의 개념으로써 개인정보 보관 및 관리의 주체가 기업이 아닌 고객 스스로가 된다. 고객들은 자신의 개인 정보를 개인스토리지(e.g. 모바일, PMP 등)에 저장한다. 고객들이 VRM 모델을 통해 개인화서비스를 받으려면, 자신의 개인 스토리지(storage)로부터 개인정보를 기업에 제공해야 한다. 이때 기업과 개인고객 사이에는 중간 브로커 서버가 존재하며 개인은 이곳에 자신의 개인정보를 올린다. 경매를 생각하면 쉽게 이해를 할 수가 있는데, 개인이 자신이 원하는 서비스 종류와 자신이 제공할 수 있는 개인정보들을 브로커 서버에 올리면, 관련 기업들은 사용자가 올린 조건들을 검토한 후에 적합한 고객을 선택한다. 사용자는 자신에게 입찰한 여러 기업들 중 자신이 원하는 서비스를 제공하는 기업을 선택하여 서비스를 받을 수 있다.

VRM의 장점은 개인이 자신의 정보를 자신이 보관하고 관리할 수 있다는 점에서 적극적 성격의 프라이버시 보호인 자기정보통제권을 강화할 수 있다는 점이다. 또한 한 사람의 개인스토리지에는 그 사람의 모든 활동정보가 저장될 수 있으므로 기존 CRM형보다 더욱 정교한 개인화서비스가 가능하다. CRM 모델에서는 개인정보의 수집이 특정 도메인의 특정 서비스로 제한되지만, VRM은 한 개인의 모든 개인정보가 도메인, 서비스의 제한 없이 개인스토리지에 수집, 저장되어 제공될 수 있기 때문이다.

비록 VRM이 고객들의 자기정보통제권을 강화할 수 있고 개인화서비스의 수준도 향상시킬 수 있지만, 이는 사용자 중심의(user-centric) 모델이기에 기업의 입장에서는 적용이 어려울 수 있다. VRM 모델에서 기업은 수동적인 정보수신자가 된다. 적극적으로 고객을 관리하고 유치해서 이익을 증대시켜야 할 기업이 개인들이 제공하는 정보를 수동적으로 취하는 VRM을 적용하기는 쉽지 않을 것이다. 개인화서비스를 제공하는 데 있어 기업의 경쟁력은 개인정보를 얼마만큼 가지고 있고, 그것을 어떻게 활용하는가에 달려 있다. VRM은 기업의 경쟁력인 개인정보의 저장, 관리를 고객에게 위임한다. 이는 기업의 경쟁력을 상실시킬 수 있다. VRM은 프라이버시 문제 해결을 위해서 아주 적절한 모델이지만 앞서 말한 기업의 경쟁력 상실 문제를 대체할 수단을 찾아내지 못한다면 그 적용은 제한적일 수밖에 없을 것이다((그림 2) 참조).



<자료>: http://netmesh.info/jernst/Digital_Identity/doc-searls-vendor-relationship-management.html

(그림 2) VRM 개념도

Ⅲ. 관련 기술 동향

개인화서비스를 위한 개인정보보호기술은 대표적으로 익명화 기술 및 프라이버시 협상 기술이 있다. 먼저 익명화 기술은 사용자와 사용자의 트랜잭션간의 연결성(linkability)을 제거해주는 기술이다. 기업은 개인정보를 수집할 수는 있지만, 어떤 사용자가 제공한 것인지는 알 수 없다. Shaffer와 Odgen은 익명성을 은밀한 정보공개를 촉진하는 요인으로 보았다[4]. 유비쿼터스 환경이 되면 더욱 민감한 정보의 제공이 이루어져야 하며, 익명화 기술의 필요성은 증대될 것이 분명하다.

또 하나의 대표기술 중 하나인 프라이버시 협상 기술은 개인의 자기정보 통제권을 강화하기 위해 필수적인 기술이다. 현재 대부분의 개인화서비스 형태가 CRM 모델임을 가정하면, 개인정보의 수집은 항상 서비스제공자가 주체가 되어 이루어진다. 서비스를 이용하려는 고객들은 서비스제공자가 요구하는 개인정보를 입력할 수 밖에 없다. 입력을 하지 않으면 서비스를 이용하지 못하기 때문이다. 프라이버시 협상은 이렇게 일방적인 정보제공을 예방하고 사용자로 하여금 자기정보의 노출 수위를 스스로 정하게 함으로써 프라이버시 침해 소지를 줄일 수 있다.

이번 절에서는 위의 두 가지 기술에 대해 장, 단점을 분석해 본다.

1. 익명화 기술

서비스제공자들은 개인화서비스를 위해 개인정보를 수집해야 한다. CRM 모델 혹은 VRM 모델 모두 개인정보는 수집되고 또 분석된다. 이렇게 수집 및 분석되는 정보를 수집하는 데 있어 사용자를 인증(authentication)하여 수집한다면 사용자는 민감한 개인정보에 대한 공개를 꺼려할 것이다. 유비쿼터스 환경에서는 사용자의 위치정보, 신체정보 등의 민감한 정보가 수집되고 그에 따른 고도의 개인화서비스가 가능해질 것이다. 하지만 이때 수집되는 정보로 인하여 사용자의 프라이버시가 침해된다면 사용자는 이러한 개인화서비스를 받으려 하지 않을 것이다. 예를 들어 범죄 및 응급상황에 신속하게 대응하기 위해 사용자의 위치정보를 실시간으로 수집하여 사용자보호 서비스를 한다고 하자[4]. 만약 이것이 오용된다면 사용자의 이동경로가 파악될 수 있으며, 이는 심각한 프라이버시 침해이다. 이러한 오용을 방지하기 위해 익명화 기술이 사용될 수 있다. 위치정보를 수집할 때 사용자의 인증이 아닌 식별(identify)만을 한다면 이동경로와 사용자간의 linkability가 제거되어 프라이버시 침해는 감소할 수 있다. 이렇게 사용자의 익명성 보장은 민감한 정보의 노출에 대한 피해를 줄일 수 있으며 이에 따라 사용자의 정보 노출 수위를 높일 수 있다.

익명화 기술은 암호학적(cryptographic)으로 구현된다. 대표적으로 그룹서명(group signature)이 있으며 본 고에서는 링 서명(ring signature), 타임캡슐을 이용한 Camenisch의 스키마를 포함하여 소개하도록 한다.

가. 그룹 서명

David Chaum과 Eugene van Heyst가 처음 소개한 개념이다[5]. 특정한 사용자 그룹을 만들고, 그룹 내의 멤버는 익명성을 보장 받을 수 있는 기술이다. 그룹에 멤버를 추가하거나, 또는 삭제할 수 있는 그룹매니저가 존재하고, 그룹의 멤버들은 멤버십 인증서와 비밀키를 그룹매니저로부터 받아 서명을 함으로써 익명성을 보장 받는다. 익명성(anonymity)은 그룹매니저만이 폐기(revocation)할 수 있고, 검증자는 서명자가 어떤 그룹에 속한지는 알 수 있지만, 누군지는 알 수 없다. 서비스 제공자의 관점에서 보면 그룹매니저가 있음으로 해서 추적성(traceability)을 보장 받을 수 있고, 사용자의 책임(accountability)도 보장 받을 수 있다.

나. 링 서명

Ron Rivest, Adi Shamir, Yael Tauman이 처음 소개한 개념이다[6]. 서명을 한 사용자가 어떤 그룹

에 속한지는 알 수 있지만, 누군지는 모른다는 점에서 그룹 서명과 같다. 단지 ring signature에는 그룹 매니저가 존재하지 않는다. Ring signature는 서명자가 그룹에 속한 사람들의 공개키만 알면 서명할 수 있으므로 그룹멤버를 추가하거나 삭제할 필요가 없고, 익명성 폐기는 서명을 생성한 자만이 할 수 있다는 특징이 있다. 단점으로는 그룹멤버의 수에 따라 서명길이가 길어진다는 것이다[7]. 개인화서비스의 관점에서 보면, 이것은 완전한 익명성을 제공한다. 즉 서비스제공자는 사용자의 실제 신분을 밝힐 방법이 없다. 이는 사용자의 입장에서는 강력한 프라이버시 보호가 될 수 있지만, 서비스제공자 입장에서 보면 잘못된 개인정보의 입력이나 의무사항의 불이행 등을 초래할 수 있다.

다. Camenisch's Scheme

Jan Camenisch 등은 여러 가지 암호학적 기법들을 사용하여 accountable privacy에 대한 시스템을 제안하였다[8]. 이 시스템은 프라이버시를 지켜줄 수 있는 익명성을 제공하는데 제한된 시간을 가정한다. 이를 위해 타임캡슐이라는 개념을 소개하는데, 타임캡슐은 일정한 기간 동안은 익명성을 유지하여 주지만, 그 기간이 지나면 사용자의 실제 신분을 서비스제공자가 알 수 있도록 하는 일종의 암호문 형태로 구성된다. Revocation authority와 신뢰된 time server, 의무이행여부를 확인해 주는 satisfaction authority 등으로 시스템을 구성하고, ZKP, VE, IBE 등의 암호학적 기법들을 사용한다. 기존의 그룹서명과 가장 큰 차이점은 익명취소를 하기 위한 근거를 암호학적으로 보장함으로써 법적인 분쟁요소를 줄였다는 것이다. 이는 현실적인 비용문제를 해결하고 익명화 기술의 보급에 도움을 줄 수 있다는 데 의의가 있다고 할 수 있다.

2. 프라이버시 협상 기술

프라이버시 협상 기술은 익명화 기술과 더불어 개인정보 보호를 위한 또 하나의 중요한 기술이다. CRM 모델에서와 같이 기업이 일방적으로 정보를 수집하고, 사용자는 수동적으로 정보를 제공하는 상황에서 사용자의 자기정보통제권은 보장받지 못한다. 프라이버시 협상은 이러한 기업주도적인 개인정보 수집으로부터 개인의 자기정보통제권을 보장해 주는 기술이다. 프라이버시 정책(privacy policy)을 이용하여 기업은 개인정보에 대한 수집요구사항을, 사용자는 자신의 개인정보 노출수위를 정하고, 그것을 교환함으로써 기업이 일방적으로 행할 수 있는 정보 수집을 예방해 준다. 프라이버시 협상을 위한 기술은 P3P, EPAL, XACML 등이 있으며[9] 그 중 대표적인 것이 P3P이다. W3C에서 제정한 P3P는 식품에 성분을 설명하는 라벨이 붙는 것처럼 특정 웹 사이트의 개인정보 보호 정책을 사이트 접속자에게 알려줌으로써 개인이 자신에 관한 정보를 제공할지 여부를 결정할 수 있도록 하는 기술이다. 이때, 웹사이트에서는 HTTP 헤더 또는 링크된 XML 파일을 통해 해당 사이트에서 취급하는 개인정보의 레벨이나 성격 등을 웹브라우저에게 알려 준다. 웹 사이트들이 P3P 소프트웨어를 설치해 두면, 방문객이 일일이 고객 약관 등 관련 규정을 확인하지 않아도 손쉽게 정보제공 수준을 결정할 수 있게 된다. 또 P3P는 사용자가 웹사이트에 기대하는 정도의 프라이버시 보호가 이뤄지지 않을 경우 이를 자동적으로 보여준다[10].

위와 같이, 프라이버시 협상 기술은 사용자로 하여금 개인정보 노출 수위를 정하도록 함으로써, 자기정보통제권을 강화하였다는 점에서 의의가 있다고 하겠다.

Ⅳ. 제언

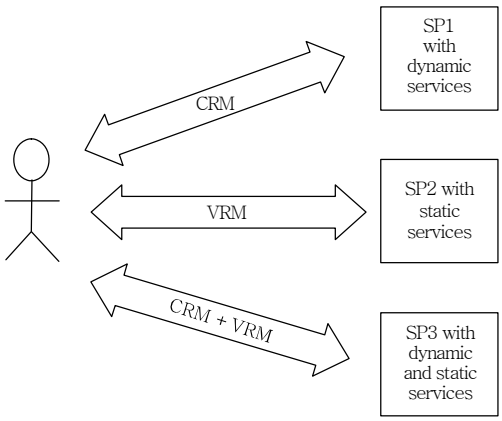
1. u-IT 환경에서의 개인화서비스 모델

유비쿼터스 환경에서는 개인정보의 수집 형태가 달라진다. 도처에 센서들이 있고 이들은 실시간으로 개인정보를 수집하여 중앙서버로 전송한다. 수집되

는 개인정보의 민감도는 높아질 것이며, 실시간 정보수집으로 인하여 사전 동의절차 이외의 실시간 동의절차가 필요할 것이다.

유비쿼터스 환경은 이러한 프라이버시 침해의 위협의 증가에도 불구하고 기존과는 다른 다양한 개인화서비스가 가능하기 때문에 의미가 있다. 예를 들어 u-Healthcare 서비스는 개인의 신체정보를 실시간으로 수집, 분석함으로써 실시간 건강체크 및 응급상황시 신속한 대응을 할 수 있는 기존에는 불가능했던 새로운 의료서비스이며, 유비쿼터스 환경에서만 가능한 개인화서비스라고 할 수 있다. 이 서비스를 위해서는 실시간으로 개인의 신체정보 및 위치 정보가 수집되어야만 한다. 이는 기존의 온라인 서비스들이 수집했던 개인정보에 비해 매우 민감한 정보라고 할 수 있으며, 따라서 프라이버시 침해의 소지가 아주 크다고 할 수 있다. 기업이 의료서비스를 목적으로 개인정보를 수집한다고 하나, 자신의 신체정보 및 위치정보가 노출된다는 것은 심각한 프라이버시 침해가 될 수 있으며, 사전 동의뿐 아니라 실시간 동의절차를 두어 해결할 수 있도록 해야 한다.

이러한 유비쿼터스 환경의 개인화서비스를 위한 개인화서비스 모델은 어떤 형태일까? 위의 u-Healthcare 서비스는 CRM 모델이라고 할 수 있다. CRM의 단점으로 지적되었던 개인의 자기정보 통제권 부재의 문제는 여전하다. 여기에 VRM 모델을 적용한다면, 자기정보통제권을 강화할 수 있다. 자신의 신체정보를 자신의 개인스토리지에 수집되도록 하고, 원하는 의료서비스에 대해 브로커서버에 요청서를 냄으로써 가능하다. 하지만 이는 실시간 서비스에는 적합하지 않다. 응급상황 대응과 같은 실시간 서비스를 받기 위해서는 서비스제공자 측의 개인정보 수집행위가 지속적으로 이루어져야 한다. 이처럼 CRM과 VRM은 완벽한 것이 아니며, 상호보완적인 관계에 있다. 유비쿼터스 환경에서는 실시간 정보를 바탕으로 하는 개인화서비스는 CRM을, 실시간 정보의 요구가 상대적으로 덜한 개인화서비스에는 VRM을 적용하도록 하는 hybrid형 모델이 필요하다((그림 3) 참조).



(그림 3) Hybrid형 개인화서비스 모델

2. 관련 기술의 문제점 및 개선 방안

가. 익명화 기술

유비쿼터스 환경의 개인화서비스를 위한 위치정보, 신체정보 등의 민감한 개인정보를 수집하기 위해 익명화 기술은 필수적인 기술이다.

하지만 완벽한 익명성 보장은 사용자로 하여금 책임을 상실하게 한다. 이는 잘못된 정보의 제공으로 이어질 수 있다. Ⅲ장 1절에서 예로 들었던 사용자 위치정보를 이용한 범죄예방 서비스를 보자. 사용자의 프라이버시를 위해 위치정보를 익명으로 수집하는 것은 당연하다. 하지만 이를 악용하여 서비스를 필요로 하지 않는 사람들이 거짓으로 서비스를 요청한다면, 진정 서비스를 원하는 사용자들은 서비스를 받기 어려워질 수 있으며, 이를 해결하기 위해 서비스제공자 측의 인력을 늘리는 것은 비용적 소모가 크다. 이러한 딜레마를 해결해 줄 수 있는 것이 바로 취소가능한 익명성(revocable anonymity), 책임있는 프라이버시(accountable privacy) 등으로 명명되는 익명취소 기술이다. 앞서 설명한 몇 가지 익명화 기술 중에 그룹서명과 Camenisch의 시스템은 익명취소도 가능한 기술들이다. 먼저 그룹서명은 그룹매니저에게 익명취소의 권한이 있다. 하지만 그룹매니저는 익명취소의 근거를 가지고 익명취소를 해

야 한다. 사용자와 서비스제공자 사이의 익명취소 근거는 물론 사전에 상호 동의 하에 정해지겠지만, 이는 분쟁의 소지가 있으며 해결을 위해 법적 절차가 필요하게 된다. 하지만 이는 시간적, 비용적 소모가 있으므로 실시간 서비스의 요구가 많아지는 유비쿼터스 환경에 적합하지 않다. 따라서 실시간으로 그리고 법이 아닌 기술적으로 명백하게 익명취소를 할 수 있도록 해야 하며, Camenisch의 타임캡슐 개념은 이를 가능하게 해줄 수 있을 것으로 보인다. 비록 Camenisch의 방법이 실제 적용되기 위해서는 많은 수정 및 보완이 필요하겠지만, 기술적으로 익명취소의 근거를 만들어 명백하고 분쟁의 소지 없이 익명취소를 하도록 하는 것은 익명성의 악용을 막고, 사용자의 책임을 강화하여 유비쿼터스 환경에서 고도의 개인화서비스를 가능하게 해줄 수 있을 것이다.

나. 프라이버시 협상 기술

프라이버시 협상 기술은 일방적인 개인정보 수집으로부터 사용자의 자기정보통제권을 강화시켜 줄 수 있는 기술로써 매우 중요한 기술임에 틀림없다. 대표적인 기술 표준 중 하나인 P3P는 사용자와 서비스제공자간의 정책교환을 통해 사용자가 서비스제공자의 정책을 알 수 있으며 협상 실패시 정보를 제공하지 않을 수 있다.

이렇게 사용자의 자기정보통제권을 강화하고자 만들어진 P3P는 지난 2002년 국제표준으로 승인이 되었지만, 현재 P3P는 널리 사용되지 않고 있다. 그 이유는 여러 가지가 있다. 첫째, 쿠키 설정의 번거로움이다. 쿠키에 대해 잘 알지 못하는 사용자들은 쿠키설정을 고수준으로 하여 매번 팝업창이 뜨는 것을 좋아하지 않을 것이다. 따라서 사용자들은 자신에게 구체적인 위협이 느껴지지 않는다면 P3P의 보안수준을 최저로 설정하게 된다. 이는 프라이버시 협상의 의미가 사라지게 되는 결과를 낳게 된다. 둘째, 프라이버시 기준 설정의 어려움이다. P3P는 사용자의 프라이버시에 대하여 고지와 선택(notice&consent)이라는 방법을 취하고 있다. 이는 사용자가 스스로 프라이버시의 기준을 세우고 이에 따라 정보제공 여부를 판단하는 방법이다. 하지만 이는 공정한 정보처리를 기대하기 힘들며, 서비스를 제공받기 위해서 프라이버시 보호수준이 아닌 포기수준을 정하는 것과 다를 바 없다[11]. 간단히 말하면, P3P는 사용자의 편의성을 고려하지 않았고, 실질적인 협상이 아닌 notice&consent를 통한 법적 절차 준수에 초점이 맞추어져 있다. 이로 인해 P3P는 사용자 프라이버시 보호가 아닌 서비스제공자의 합법적인 개인정보수집을 위한 도구로 전락하게 되었다.

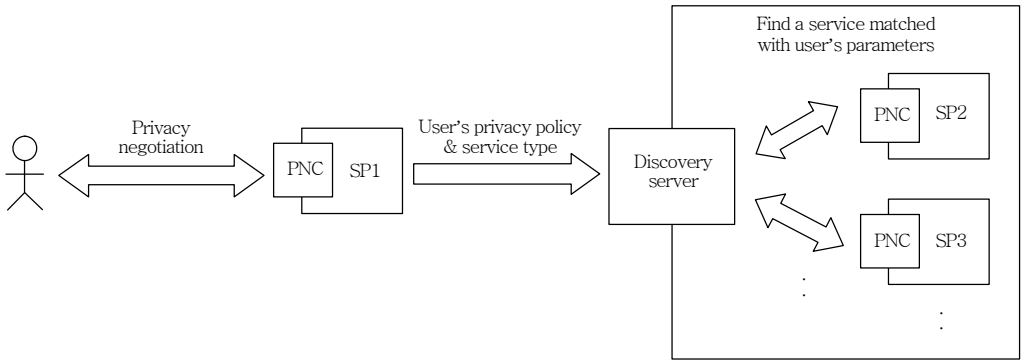
본 고에서는 위와 같은 문제점을 해결할 수 있는 새로운 프라이버시 협상의 개념을 설명하고자 한다. 프라이버시 협상의 문제점은 정책교환 이후에 notice&consent 절차를 통해 정보노출 수위를 정한다는 것이다. 이는 사용자의 동의를 통한 개인정보 수집이라는 법적 절차를 지킨다는 점에서, 법적으로는 사용자의 자기정보통제권을 지켜주는 것처럼 보일 수도 있다. 하지만 이는 실질적인 프라이버시 협상이 아니며, 사용자는 서비스를 제공 받기 위해 자기정보의 노출을 법적으로 허용하는 것이다. 사용자가 프라이버시 협상 기술을 통해서도 자신의 정보를 보호하지 못하는 이유는 다음과 같다.

- 프라이버시 협상이 실패할 경우, 사용자는 해당 서비스를 제공 받지 못한다. 서비스를 이용하기 위해서는 자신의 정책을 변경하여 서비스제공자가 원하는 정보를 제공하거나, 다른 서비스를 찾아야 한다.

사용자는 서비스제공자에 비하면 약자(弱者)이다. 사용자가 자신이 원하는 서비스, 자신의 정책과 일치하는 서비스를 받기 위해서는 디스커버리(discovery) 시스템이 필요하다. 프라이버시 협상이 실패하더라도 원하는 서비스를 자동으로 찾아주는 시스템이 있다면, 사용자는 더 이상 서비스제공자의 정책에 맞추지 않고, 자신의 정책을 고수(固守)할 수 있을 것이다.

제안하는 디스커버리 시스템은 (그림 4)와 같이 구성될 수 있다.

사용자와 서비스제공자1(SP1)의 협상이 실패할



(그림 4) 디스커버리 시스템을 이용한 프라이버시 협상 기술

경우, 서비스제공자1의 프라이버시 협상 컴포넌트(PNC)는 디스커버리 서버를 호출한다. 그리고 디스커버리 서버에 사용자의 프라이버시 정책 및 서비스 종류를 전달(toss)하고 디스커버리 서버는 이 정책을 바탕으로 다른 서비스제공자들의 프라이버시 정책 및 서비스 종류를 비교하여 사용자의 정책과 맞는 정책을 찾아준다. 이때 서비스제공자들은 자신들의 정책, 제공하는 서비스의 도메인, 종류 등을 명시해주어 디스커버리 서버의 검색시간을 줄일 수 있도록 한다. 이로써 사용자는 자신의 프라이버시 정책과 서비스제공자의 프라이버시 정책이 맞지 않는 경우에도 자신이 원하는 대체서비스를 검색하여 이용할 수 있게 됨으로써 실질적인 자기정보통제권을 보장 받을 수 있게 될 것이다.

V. 결론

본 고에서는 개인화서비스를 위한 개인정보 수집 및 이용모델과 관련 기술들을 분석하여 유비쿼터스 환경에서 적용할 수 있는 새로운 모델과 기술들을 제시하였다.

첫째, 개인정보 수집 및 이용모델은 크게 CRM과 VRM이 있다. CRM은 개인정보의 수집과 이용의 주체가 기업이며, VRM은 사용자가 된다. 이들은 각각 장단점을 가지며, 어느 하나만을 가지고 완벽한 개인화서비스를 할 수 없다. CRM은 기업의 이익 및 경쟁력 확보를 위해, VRM은 사용자의 자기정보통제권 강화 및 고도의 개인화서비스를 위해 필요하며 유비쿼터스 환경에서 이들은 양립하여 상호보완적으로 운용되어야 할 것이다.

둘째, 개인정보 수집 및 이용 모델에 필요한 요소기술 중 익명화 기술과 프라이버시 협상기술에 대해 분석해 보았다. 익명화 기술은 사용자가 민감한 개인정보를 제공할 수 있도록 하여 고도의 개인화서비스를 가능하게 하는 반면, 사용자에 따라 악용될 소지가 충분히 있으므로 책임을 강제할 수 있는 방안이 필요하다. 그리고 프라이버시 협상기술은 사용자의 자기정보통제권을 강화하기 위한 필수기술 중 하나이며, 실시간 서비스가 가능하고 도처에서 정보수집이 일어날 수 있는 유비쿼터스 환경에서 꼭 필요한 기술 중 하나라고 할 수 있다. 하지만 현재의 프라이버시 협상 기술은 문제점이 많아 실제 사용이 미비하며, 이에 본 고에서는 새로운 프라이버시 협상 모델을 제안하여 문제점을 해결하고자 하였다. 제안한 프라이버시 협상 모델은 프라이버시 협상이 실패하더라도 대체 서비스를 찾을 수 있도록 디스커버리 시스템을 이용하도록 한다. 이로써 사용자는 자신의 프라이버시 정책을 서비스제공자의 프라이버시 정책과 맞출 필요가 없어지게 되며, 이는 실질적인 자기정보통제권의 강화로 이어질 수 있을 것이다.

본 고에서 제안한 모델과 관련 기술들은 유비쿼터스 환경에서 안전하고(secure) 고도화된(advanced) 개인화서비스를 실현하는 데 도움을 줄 수 있을 것으로 예상된다.

● 용 어 해 설 ●

식별(Identification): 사전적으로는 생체·사체 또는 그 일부를 대상으로 개체의 이동(異同)을 식별하는 일이며, 웹에서의 식별은 보통 identifier를 통해 가입자를 구분하는 것을 말함

인증(Authentication): 사전적으로는 어떠한 행위 또는 문서의 성립·기재가 정당한 절차로 이루어졌음을 공적 기관이 증명하는 일이며, 웹에서의 인증은 보통 identifier를 통해 식별된 대상이 실제로 identifier를 등록했던 대상이 맞는지 확인하는 일을 말함

책임(Accountability): 사용자가 익명성을 악용하지 않고 올바른 정보만을 제공하는 것을 말함

Notice&Consent: 개인정보보호법에는 개인정보를 수집할 때, 수집 목적, 이용 범위, 정보주체의 권리 등을 명시하도록 하고 있다. 현재 많은 웹사이트들은 개인정보를 수집할 때, 위의 사항들을 약관으로 구성하여 사용자에게 보여주고(notice), 사용자는 이에 동의(consent)하는 형태를 취하여 개인정보를 수집하고 있음

쿠키(Cookies): 인터넷 웹사이트의 방문기록을 남겨 사용자와 웹사이트 사이를 매개해주는 정보를 말함

약어 정리

CRM	Customer Relationship Management
EPAL	Enterprise Privacy Authorization Language
IBE	Identity Based Encryption
P3P	The Platform for Privacy Preferences
PNC	Privacy Negotiation Component
VE	Verifiable Encryption
VRM	Vendor Relationship Management
XACMA	eXtensible Authorization Control Markup Language
ZKP	Zero Knowledge Proof

참 고 문 헌

[1] 이준기, 최희재, 최선아, "서비스의 유용성과 프라이버시 염려도가 개인화된 서비스 수용성에 미치는 영향에 관한 연구," 한국전자거래학회지, 제12권 제4호, 2007.

[2] "고객관계관리," http://www.terms.co.kr/CRM.htm

[3] 오상진, "위치정보서비스, 진흥과 규제 이슈," TTA 저널, No.123, 2009.

[4] 김범수 외 10인, "개인정보 보호 및 이용의 현황과 사례," 한국학술정보, 2008.

[5] David Chaum and Eugene van Heyst, "Group Signatures," EUROCRYPT'91, 1991.

[6] Ronald L. Rivest, Adi Shamir, and Yael Tauman, "How to Leak a Secret," ASIACRYPT2001, LNCS 2248, 2001, pp.552-565.

[7] 이윤경, 한승완, 이석준, 정병호, 양대헌, 권태경, "익명인증 기술과 동향," ETRI, 전자통신동향분석, 제23권 제4호, 2008. 8., pp.19-29.

[8] Jan Camenisch, Thomas Groß, and Thomas S. Heydt-Benjamin, "Rethinking Accountable Privacy Supporting Services," DIM2008, 2008.

[9] 노종혁, 진승헌, "웹 환경에서 정책 기반 개인정보보호 기술," 전자통신동향분석, 제2권 제4호, 2007. 8., pp.144-155.

[10] P3P, http://www.juhorang.com.ne.kr/study/sisa/p3p.htm

[11] 윤재석, "P3P 논의 현황과 문제점 및 국내정책 방향," KISA, 2004.