DOI: 10.3745/KIPSTC.2010.17C.2.135

u-City환경에서 맞춤형 서비스 제공을 위한 프로파일기반 개인 정보보호 관리

이 준 규[†] · 김 지 호[††] · 송 오 영[†††]

요 약

u-City에서는 도시 곳곳의 센서를 통해 상황정보를 수집하고, 사용자의 요청에 의해서가 아닌 그 상황에 필요한 서비스를 자동적으로 제공하게 되는 서비스 개인화를 추구한다. 그러나 맞춤형 서비스를 제공하기 위해서는 다양한 센서를 통해 수집되는 상황정보를 필요로 하게 되는데, 이와 같은 상황정보에는 개인의 프라이버시 정보를 포함한다. 따라서 서비스 제공으로 인한 편리성과 정보보호라는 측면 사이에서 적절한 조율 내지는 관리가 필요하다.

본 논문에서는 맞춤형 서비스 환경에서 요구되는 다양한 개인의 상황정보를 분류하여 등급화 하였고, 이를 기반으로 사용자 프로파일(User Profile)과 서비스 프로파일(Service Profile)간의 프로파일 매칭(Profile Matching)을 통해 서비스 제공여부를 결정하고, 전달되는 개인정보의 암호화, 이를 위한 키 분배를 관리하는 정보보호 관리를 제안한다.

키워드 : 상황인지, 개인정보, 프로파일, 보안, 유비쿼터스 도시

Privacy Management Based on Profile for Personalized Services in u-City

Jun-gyu Lee[†] · Ji-ho Kim[††] · Oh-young Song[†††]

ABSTRACT

U-City pursues personalized service by collecting contexts through sensors located over the city and presenting the service automatically depending not on the user's request but on the situations that are needed. To provide the personalized service, however, contexts collected through various sensors are needed, and they include private information. Therefore, it is important to keep a balance between the convenience by presenting service and protecting private information.

In this paper, we classify and grade person's various contexts requested in the personalized service environment. Based on these, we make decisions on whether to present the service or not by profile-matching between user profile and service profile. Also, we propose an efficient privacy-protection management scheme to encrypt transmitted private information and to control key distribution.

Keywords : Context-Awareness, Privacy, Profile, Security, u-City

1. 서 론

수 년전만 하더라도 낯설기만 했던 '유비쿼터스'란 용어는 이제 실생활 곳곳에서 흔히 쓰이는 보통명사가 되었다. 더욱이 우리나라는 세계 최고의 IT인프라를 기반으로 유비쿼터스 컴퓨팅 기술이 하루가 다르게 발전하고 있으며, 유비쿼터스에 관해선 우리나라의 확산 속도를 어느 나라도 따라오지 못한다. 이제 우리나라는 미래형 첨단도시, u-City(ubiquitous-City)구현을 현실화하고 있다. 인공지능에 의해 도로와 교통상태가 관리되고, 공장 유해가스 배출, 소음정도 등을 실시간으로 점검하며, 주변지역의 각종 치안 범죄를 실시간으로 모니터링해 안전한 도시환경을 보장하는 u-City 구현은 우리에게 장밋빛 미래를 약속하면서 동시에 정보화 사회에서 유비쿼터스 사회로의 변화를 예고하고 있다.

u-City란 주거, 산업, 문화, 행정, 환경 등에 대한 도시 기능을 효율적이고 체계적으로 구현하기 위해 도시 기획의 초기 단계부터 IT기술과 정보통신 인프라를 반영하여, 정보화에 따른 도시 생활의 편의를 도모하고 삶의 질 향상, 체계적인 도시 관리에 의한 안전과 주민복지 향상 등 도시의 기능을 획기적으로 진보 시킬 수 있는 도시로 정의 된다.[1]

※ 본 연구는 서울시 산학연 협력사업(CR070019) 지원으로 수행되었습니다.
† 준 회 원 : 중앙대학교 전자전기공학부 석사과정
†† 정 회 원 : 중앙대학교 전자전기공학부 연구교수
††† 정 회 원 : 중앙대학교 전자전기공학부 교수
논문접수 : 2008년 6월 27일
수 정 일 : 1차 2008년 11월 13일, 2차 2009년 4월 14일
심사완료 : 2009년 5월 19일

u-City환경에는 광대역통합망(BcN), 전자태그(RFID), 위치기반서비스(LBS), WiBro, 위성위치추적시스템(GPS), 유사광가입자망(FTTP), 홈 네트워크 등 다양한 유비쿼터스 IT기술들이 총망라되며 이러한 기술을 기반으로 쾌적한 도시, 편리한 도시, 안전한 도시생활을 위한 각종 서비스들이 제공된다. 최근 여러 기술 개발 업체와 서비스를 제공하는 비즈니스 업체들이 우선적으로 고려하고 있는 u-City 주요 서비스를 요약하면 <표 1>과 같다.[2, 3]

이는 홈 네트워크 구축과 관련한 u-Home 서비스, 지능형 교통 시스템 구축과 관련된 u-Traffic 서비스, 의료/생명과 연관된 u-Health 산업, 미래형 도시 방범/치안 시스템 구축과 관련된 u-Security 등으로 요약할 수 있다. 이외에도 교육과 관련된 u-Education, 도시거주민에게 각종 행정 서비스를 제공하는 u-Government, 원격 근무, 자재관리를 제공하는 u-Office 등을 대표적인 u-City 서비스로 들 수 있다.[4]

향후 u-City에서는 이러한 서비스들이 더욱 지능화되어, 사용자가 직접 원하는 정보와 서비스를 요청하는 것이 아니라 사용자의 상황에 알맞은 정보와 서비스를 선별하여 제공하게 되는 맞춤형 서비스로 진화할 것이다. 이러한 상황인지형 시스템은 사용자의 정보선택을 도와주고 나아가 개인별 맞춤 서비스를 제공하므로 생산된 정보와 서비스의 효용성을 극대화시킨다. 즉, 사용자가 원하는 정보를 찾아보도록 하는 것이 아니라 사용자의 상황에 맞게 알맞은 정보를 선별하여 제공하게 되는 것이다. 이러한 관점에서 u-City의 응용 및 서비스는 컴퓨팅 및 커뮤니케이션 능력을 가진 스마트 객체(entity)들이 동적인 환경 변화를 인식하고 이에 적응할 수 있는 특성, 즉 상황인지(context-aware) 특성을 갖게 될 것이다.

상황정보는 사용자와 서비스 간에 상호 작용을 하는 시점에서 이용할 수 있는 거의 모든 정보이다. 이는 일반적으로 이름, ID같은 신원 정보, 체온, 혈압 등의 신체 정보, 위치, 속도 같은 공간 정보 등을 포함한다. 사용자의 현재 활동과 같이 개인적인 것일 수도 있으며, 현재 사용 중인 기기와 같이 기술적인 것일 수도 있고, 또한 온도, 위치, 또는 시간과 같이 환경적인 것일 수도 있다.[5] 상황인지 서비스는 이러한 상황정보의 수집 및 교환을 통해 상황을 인식하고, 해석 및 추론과 같은 처리 과정을 거쳐 사용자에게 필요한 맞춤형 서비스를 제공한다. 예를 들어 긴급 재난 서비스의 경우, A지역의 집에 불이 났다면 그 집의 화재 센서는 u-City 통합운영센터에 긴급재난요청을 보낸다. 통합운영센터는 A지역의 관할 소방서에 연락을 하고 소방차를 출동시킴과 동시에 A지역의 주민들에게 화재 소식을 알리고 u-Traffic시스템으로 정보가 전달되어 인근지역의 교통상황을 파악하여 u-Traffic서비스를 통해 그 지역을 지나는 차량들을 교통상황이 원활한 B지역으로 우회하도록 하여 소방차등이 빨리 진입할 수 있도록 한다.

〈표 1〉 u-City에서의 주요 서비스

분 야	서 비 스	분 야	서 비 스
u-Traffic	교통정보서비스 음성길안내서비스 주차정보서비스 사고예방서비스 장애인교통안내서비스 대중교통정보 서비스	u-Home	원격제어/검침서비스 홈오토메이션서비스 홈시큐리티서비스 단지안내서비스 생활정보서비스
u-Health	원격검진서비스 의료상담서비스 건강모니터링 서비스 응급환자인식서비스 생활건강정보 서비스	u-Security	약자보호서비스 비상호출서비스 화재관리서비스 하천재난감시 서비스 공공지역 영상감시서비스

이와 같이 상황인지 기반의 u-City서비스 제공 환경은 산업 및 사회에 미치는 순기능이 지대하다. 하지만 요즈음도 이슈화 되고 있는 개인정보의 침해와 관련해서 본다면 그 역기능을 심각하게 고려하지 않을 수 없다. u-City에서는 서비스 제공을 위해 필연적으로 개인에 관한 정보를 요구한다. u-City에서 요구되는 정보는 현재 정보화 사회에서 요구되는 단순한 개인의 신상정보가 아니라 생체 인식을 통해 획득되는 바이오 정보, 실시간 추적을 가능케 하는 위치정보 등의 새로운 정보이고, 또한 어떤 개인의 행동과 성향 전반에 대해 끊임없이 수집되는 민감한 정보이기 때문에 정보 주체의 프라이버시 침해 위협이 지금보다 훨씬 높아진다.[6] 또한 유비쿼터스 IT기술이 서양에서는 이처럼 감시사회에 대한 사생활 침해와 관련하여 매우 논쟁이 심한데 반해 우리나라를 포함한 아시아에서는 주로 생활편의와 복지수준향상, 경제성장과 같은 긍정적인 측면만 집중적으로 부각되고 있는 것이 현실이다. u-City구현의 세계 선두에 서 있는 우리나라도 아직 개인의 프라이버시와 정보보호, 정보통제와 관련한 부분에 있어서는 충분한 준비가 이루어지지 않은 상황이다. 따라서 개인정보유출에 대한 불안감을 해소하고, 사용자에게 신뢰도 높은 u-City서비스를 제공하기 위해 u-City 구현은 그 장점뿐만 아니라 역효과에 관하여도 심도 있는 검토가 뒤따라야 한다.

이 후 본 논문에서는 u-City구현 시 현재와 달라지는 보안환경, 정보보호의 초점을 검토하고 다양한 u-City 서비스 시나리오를 제시하여 유출 위협이 있는 개인정보를 분석한다. 또한 개인정보의 관리/보호 극대화를 위하여 다양한 개인의 상황정보를 분류하여 등급화 하였고, 이를 기반으로 개인단말에 저장되는 사용자 프로파일(user profile) 설정과 서비스 제공자(service provider)가 생성하는 서비스 프로파일(service profile)간의 프로파일 매칭(profile matching)을 통해 서비스 제공여부를 결정하고, 전달되는 정보의 암호화, 키 분배를 관리하는 효과적인 정보보호 관리에 대해서 제안한다.

2. 본 론

2.1 u-City 구현 시 보안환경의 변화

u-City환경에서는 각종 센서나 CCTV 같은 수많은 이질적 디바이스들이 컴퓨팅 기능을 내장하고 상호 네트워크로

〈표 2〉 보안환경의 변화

분 류	내 용
디바이스 측면	개인정보 침해사고의 대상이 PC와 네트워크를 포함한 무선단말, 정보가전 등 다양한 디바이스로 확대됨.
침해 가능성의 증가	개인정보의 범람으로 프라이버시 침해 위협도 커짐.
침해 유형의 지능화	비교적 보안등급이 낮은 사용자의 정보(위치, 취미생활)도 유출시 추적을 통해 그 사용자의 신원과 행동 패턴 등을 추론할 수 있음.
네트워크 측면	인터넷침해사고에 취약한 인터넷망에서 발생된 개인정보 침해위협이 BcN을 통해 통신망, 방송망 및 USN까지 확산 가능.

연결되어있다. 따라서 정보보호의 대상이 시스템이나 네트워크에서 개별 디바이스로 확대되어야 한다. 또한 u-City안에는 위치센서, CCTV, 온도/습도 센서등 사용자의 상황을 인지하기 위한 수많은 단말들이 거미줄처럼 얽혀있게 된다. 때문에 전달되는 정보의 양이 방대해 지고, 도청을 통한 개인정보의 유출 가능성이 지금보다 더 높다. 마지막으로 u-City안에서 전달되는 개인정보의 특성을 보면, 현재의 단편적이고 개인의 신상에 관련된 정보들로 국한되는 정적인 개념이 아니라 실시간으로 변동되는 위치, 체온, 속도 등의 동적인 정보이며 개인의 신원정보와는 연관성이 없는 상황정보까지 포함하는 개념으로 확대된다. 예를 들어, 개인의 위치정보, 목적지 정보 등은 특정 개인을 식별하는 정보가 아니고 또한 일회성의 성격이 강하나 이를 주기적으로 수집한다면 그 사람의 행동패턴을 분석가능하고 나아가 신원을 추적할 수 있게 된다. 이와 같은 보안환경의 변화를 정리하면 <표 2>와 같다.

2.2 u-City 제공 서비스와 유출 가능 개인정보

u-City환경에서 다양한 서비스가 제공될 때, 각 서비스는 사용자의 모든 상황정보를 필요로 하는 것은 아니다. 예를 들어 시각장애인이 u-Traffic/음성 길안내 서비스를 이용할 때, 서비스 제공자는 처음에 그 사람의 장애정보와 위치정보를 검색하여 서비스를 실행하게 되고, 이 후에는 위치정보만 가져오면 원활한 서비스 제공이 가능하다. 이를 보안의 관점에서 본다면 서비스 제공에 필요한 사용자의 상황정보는 곧 서비스 제공시에 유출 가능한 정보라고 생각할 수 있다. 아래의 <표 3>은 u-City 서비스 이용 시나리오를 토대로 각 서비스 별 유출 가능한 정보들을 보여준다.

2.3 개인상황정보의 등급화

u-City의 도시거주민에게 <표 3>과 같은 서비스를 제공하기 위해서 요구되는 정보는 개인의 바이오정보, 위치정보 등 민감한 정보가 있고, 반면에 나이와 같은 통계나 연구목적의 상대적으로 그 민감성이 적은 정보도 있다. 따라서 사용자 프라이버시침해를 최소화하기 위해서는 개인상황정보의 등급화와 그에 따른 적절한 관리가 필요하다. 어떤 정보는 공개적 접근이 허용되어야 하고, 어떤 정보는 보다 철저하게 보호되어야 한다. 예컨대 개인상황정보에는 의료, 성적 취향과 같이 수집이나 공개가 절대적으로 제한되는 정보가 있고, 수집과 이용 및 공개에 반드시 당사자의 동의 또는 통지를 요하는 정보도 있을 것이다. 개인상황정보의 등급화는 그러한 판단을 내리는데 없어서는 안 될 것이다. 또한 정보의 수명 관리에도 개인상황정보의 등급화는 필수적이다.[7]

본 논문에서는 u-City 서비스 제공시 전달되는 개인상황정보를 그 민감성에 따라 (그림 1)과 같이 4등급으로 분류하였다. 분류의 기준이 되는 개인상황정보의 민감도는 특정 개인을 식별할 수 있는 정보인지 여부와 유출시 개인 또는 사회에 미칠 수 있는 부작용을 고려하여 판단하였으며 각 보안레벨별 세부 분류기준은 다음과 같다.

먼저 가장 민감도가 낮다고 판단한 보안레벨 1(level 1)의 개인상황정보를 보면, 이들은 복수의 정보가 유출되어도 특정개인을 식별하기가 힘든 정보들로 구성되지만 다량 유출시 상업적인 조사(調査)나 통계목적으로 이용될 소지가 있는 것들이다. 또 보안레벨 2의 정보들은 역시 한 가지 항목의 정보수집만으로 특정개인을 식별하기가 어려우나 같은 레벨의 다른 정보들과 결합하면 특정개인을 용이하게 추출할 수 있는 상황정보들로 구성된다. 보안레벨 3은 특정개인을 식별 가능한 정보들이 주를 이루며, 여기에 사적인 비밀, 치부(恥部)로 간주할 수 있는 정보들도 이 레벨에 속한다. 마지막으로 민감도가 가장 높다고 판단한 보안레벨 4로 분류된 개인상황정보의 경우, 유출 되었을 시 특정개인의 식

〈표 3〉 시나리오별 유출가능 개인정보 유형

서비스 분야	서비스 이용 시나리오	노출 가능 개인정보
u-Health (원격진료 서비스, 의료상담 서비스)	평소 당뇨병과 고혈압 증상이 있는 독거노인 A씨는 아침마다 일어나서 자신의 건강 리포트를 읽는다. 취침하는 동안 침대에 내장된 건강 센서는 혈압, 맥박, 체온 등을 체크하여 병원으로 송신하였고, 병원에서는 이 정보를 수집/분석하여 결과를 A씨에게 보내준 것이다.	체온, 맥박 등의 신체 상황정보나 병력(病歷), 진단기록 등이 유출될 위험이 있다.
u-Biz (맞춤형 News 서비스)	의류회사에 다니고 있는 B씨는 수시로 자신의 PDA 단말을 통해 전자신문을 읽는다. PDA 단말은 실시간으로 관련업계 동향이나 신제품 소식을 다운로드하여 B씨에게 알림메시지를 통보해준다.	직업이나 근무지, 직책 등의 정보가 유출될 수 있다.
u-Biz (자동결재 서비스)	저녁 6시, 가족의 저녁식사 준비를 위해 근처 대형마트에 간 C씨는 평소에 남편과 아이들이 좋아하는 식품을 골라 계산대로 향한다. 계산대의 자동결재시스템은 각 식품에 부착된 태그와 정보를 교환하고, 대금은 사전에 등록된 C씨의 신용카드에서 실시간 지불된다.	행동패턴이나 기호식품, 소비력 등이 노출될 수 있다.
u-Home (약자보호 서비스)	밤 11시쯤부터 D씨는 IPTV를 켠 후 학원을 마치고 귀가하는 딸의 모습을 확인한다. 도시 곳곳에 설치된 CCTV는 딸의 위치정보를 확인하여 실시간 영상을 D씨에게 송신한다.	개인의 위치나 차량의 위치, 행동패턴 등이 노출될 수 있다.

Security Level	General	Surrounding	Vital	Special	서비스 예시
LEVEL 1	나이, 성별, 종교, 기술자격 및 전문면허	주변환경 상황정보 (온도, 습도, 소음)	몸무게, 키, 피부정보, 모발, 가슴둘레	여가활동, 기호식품, 흡연, 관심사, 스포츠 및 오락	맞춤광고 서비스 상품진열안내 서비스
LEVEL 2	이름, 직업, 학력, 학교, 차량정보, 가족구성	공간상황정보 (위치, 속도, 방향)	신체상황정보(체온, 맥박, 혈당), 혈액형, 가족병력	여행정보, 목적지, 클럽 가입정보, 정당가입정보	음성길안내 서비스 생활건강정보 서비스
LEVEL 3	주민등록번호, 봉급액 사업소득, 단말번호	TBD	장애상황정보(수술, 지병, 장애등급), 개인의료기록	스케줄 정보, 보험가입 정보, 가계지출정보	약자보호 서비스 의료상담 서비스
LEVEL 4	계좌번호, 소유재산 및 부동산정보, 집주소	TBD	지문, 홍채정보, DNA	납세정보, 성생활 정보	홈시큐리티 서비스 납세정보 서비스

TBD : To be determined

(그림 1) 개인상황정보의 등급

별은 물론, 개인의 재산 또는 사회생활에 치명적인 해를 입힐 수 있는 정보들이다.

(그림 1)의 오른쪽 서비스 항목은 u-City 주요 서비스 중에서 각 보안레벨의 개인상황정보가 필수적으로 요구되는 서비스의 예시이다. 예를 들어, 생활건강정보 서비스가 사용자에게 제공되기 위해서는 보안레벨 2(level 2)의 개인상황정보 즉, 현재 사용자의 체온, 맥박, 혈당수치 등이 요구되는 것이다.

2.4 사용자 프로파일(User Profile)과 서비스 프로파일(Service Profile)

본 논문에서는 u-City안에서 전달되는 개인상황정보의 등급화를 기반으로 사용자 개인정보 프로파일과 서비스 프로파일의 매칭(matching)을 통해서 맞춤형 서비스의 제공여부를 결정하고 전송되는 개인 프라이버시 정보를 보호하도록 명령(command)하는 개인정보보호 관리 기법을 제안한다. 먼저 사용자 프로파일이란 보호되어야 하는 정도(level), 각종 상황정보의 범주(category)에 따라 분류된 개인정보와 그 개인정보가 서비스 제공을 위해 사용되어 질지의 여부를 설정 한 것이다. (그림 2)와 같은 구조이며 이는 XML의 형식으로 사용자의 개인 단말에 저장된다. 사용자는 자신의 의도에 따라 프로파일의 설정을 변경할 수 있으며 자신의 판단과 관련 서비스에 따라 개인정보의 사용 여부를 결정할 수 있다. Set up 필드의 “Open(공개)”설정은 서비스 제공을 위해 사용되어도 좋다는 것을 의미하고, “Block(보호)”설정은 정보사용/공개 거부를 나타내며 마지막으로 “Conditional (조건부)”설정은 상황에 따라 조건부 공개할 수 있는 항목을 의미한다.

그리고 이와 동시에 서비스 제공자 측에서는 서비스 공급을 위해 필요한 사용자의 상황정보가 명시된 서비스 프로파일이 존재한다. 이는 각 서비스마다 요구되는 사용자의 개인정보가 다르므로 각 서비스별로 서비스 프로파일도 따로 존재한다. 예를 들어 u-Traffic/음성 길안내 서비스의 경우에 서비스 프로파일은 (그림 3)과 같다. 이는 현재 사용자에게 날씨와 주변의 교통상황을 고려하여 목적지까지 최적의 루트를 안내해주는 서비스로서 위의 프로파일을 보면 사용자의 현재 위치나 속도, 차량정보 등이 서비스 제공에 반드시 필요하다는 것을 의미한다. 만약 사용자가 이 같은 정보를 자신의 프로파일 상에서 “Open(공개)”로 설정해 놓은 상태라면 사용자가 차량에 탑승하는 순간 상황인지 추론과정을 거쳐 사용자는 자동으로 이 서비스(맞춤형 서비스)를 제공 받게 된다.

Security Level	Category			
	General	Surrounding	Vital	Special
LEVEL 1	N/A	주변환경정보(날씨, 습도, 기온)	N/A	N/A
LEVEL 2	차량정보	공간상황정보(위치, 속도, 방향)	N/A	목적지 정보
LEVEL 3	N/A	N/A	N/A	N/A
LEVEL 4	N/A	N/A	N/A	N/A

(그림 3) 서비스 프로파일 (u-Traffic/음성 길안내 서비스)

Security Level	General	Set up	Surrounding	Set up	Vital	Set up	Special	Set up
LEVEL 1	나이, 성별, 종교, 기술자격, 면허정보	Open	주변환경 정보(온도, 습도, 소음),날씨, 시간	Open	키, 몸무게, 피부정보, 모발, 가슴둘레	Open	기호식품, 여가활동, 흡연, 스포츠 및 오락	Block
LEVEL 2	이름, 직업, 병역정보, 학력, 학교, 차량정보	Block	공간상황 정보(위치, 속도, 방향)	Open	체온, 맥박, 혈당, 혈액형, 가족병력	Cond	여행 목적지, 클럽가입 정보, 정당가입 정보	Cond
LEVEL 3	주민등록번호, 개인 단말번호, 사업소득	Block	TBD		장애등급, 수술, 지병, 개인의료기록	Cond	스케줄정보, 보험가입 정보, 가계지출정보	Block
LEVEL 4	계좌번호, 소유재산, 부동산정보, 집주소	Block	TBD		지문, 홍체, DNA	Block	납세기록	Block

TBD : To be determined

(그림 2) 사용자 프로파일

〈표 4〉 프로파일 매칭 시나리오

아침에 일어난 A씨는 자신의 PDA 단말을 확인한다. 이때 A씨가 사는 지역의 날씨, 기온 및 기상예보가 다운로드 되고, A씨는 이를 확인한다. A씨는 이와 같은 기상정보 서비스를 받기 위해 사전에 필요한 개인정보(위치, 시간정보)를 사용자 프로파일 (그림 2)와 같이 사용가능/공개로 설정해 놓았기 때문에 자동으로 이 서비스를 받게 된다. 대중교통을 이용하는 A씨는 출근길에서 주위 사람 몇몇이 개인 단말을 통해 전자신문을 읽는 것을 본다. 이는 대중교통을 이용하는 동안 사용자의 상황을 인지하여 개인의 직업이나 관심사, 취미에 따라 업계 동향이나 신제품 소식 등을 전달해주는 u-Biz/맞춤형 전자신문 서비스이다. 하지만 A씨는 출근하는 동안 자신의 단말을 통해 이 서비스를 제공받지 못한다. 서비스를 받기위해 필요한 개인상황 정보와 A씨 사용자 프로파일의 개인상황 정보 분류, 수준별 설정이 서로 매치되지 않았기 때문이다. 예를 들어 A씨는 (그림 2)와 같이 자신의 프로파일에서 취미, 직업 등의 정보는 사용불가/공개 거부로 설정해 놓았다. 회사에 도착한 A씨는 정문에서 홍채인식으로 근태를 체크하고, 자신의 자리에 앉는다. A씨의 의자에는 혈압, 맥박, 체온 등을 체크하는 건강 센서가 내장되어 있다. 이는 또한 u-Health/건강 모니터링 서비스와 연결되어 있는데 사용자가 아침에 출근했을 때, 또는 외부 출장을 다녀온 직후 등 사용자의 상황을 인지하여 적절한 시간마다 신체 정보를 체크하고 이를 병원으로 송신하여 사용자의 건강상태를 리포트 해주는 서비스이다. 하지만 이제 막 자리에 앉은 A씨는 이 서비스를 제공 받지 못했다. A씨의 프로파일 (그림 2)를 보면 이 서비스를 받기 위해 필요한 개인정보(혈압, 맥박 등 신체 상황정보) 카테고리가 조건부 사용가능/공개로 설정되어 있기 때문이다. 하지만 조건부로 설정이 되어 있는 경우, A씨의 단말에 지금 사용가능한 서비스의 내용과 이 서비스를 제공받기 위해 변경해야 하는 A씨의 프로파일 설정 항목이 메시지로 전달된다. A씨가 단말을 통해 이 메시지를 보고 프로파일 설정 변경을 동의 한다면 일시적으로 A씨 프로파일 설정이 변경되고, A씨는 몇 분후 자신의 건강상태 리포트를 받아볼 수 있을 것이다.

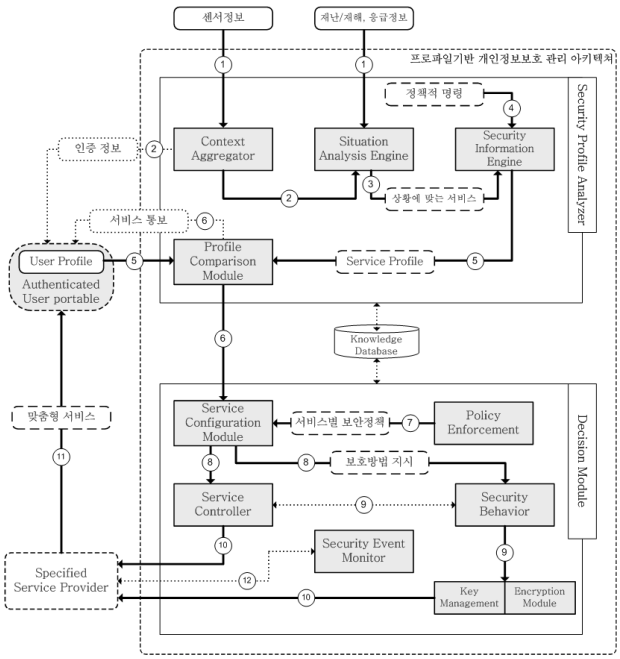
<표 4>는 앞에서 설명한 프로파일 설정을 가지고 있는 사용자가 상황인지기반 u-City 환경에서 프로파일 매칭을 통해 맞춤형 서비스를 제공받는 과정을 보여주는 시나리오이다. 시나리오에서 사용자 프로파일 설정은, 일반(General) 카테고리의 개인정보는 보안레벨 1(level 1)을 제외한 모든 정보가 “Block(보호)”로 설정되어 이들 정보가 요구되는 서비스 항목은 모두 거부/차단된 상태이고 반면에 사용자의 주변정보(Surrounding)는 모두 “Open(공개)”설정 되어있다. 또 나머지 두 카테고리 중 신체상황정보의 보안레벨 2(level 2) 항목들, 즉 체온, 맥박, 혈당 등의 정보는 “Conditional(조건부)” 설정되어 있음을 (그림 2)에서 볼 수 있다.

다음에는 위 시나리오를 실현하는 프로파일기반 개인 정보보호 관리의 세부 구조(architecture)와 전체 시스템의 흐름도에 대해서 설명하고, 이를 평가하기 위해서 테스트베드 구현을 통해 시스템의 성능을 분석해 보고자 한다.

2.5 프로파일 매칭을 통한 개인정보 보호/관리 아키텍쳐

(그림 4)는 본 논문에서 제안한 시스템의 세부 구성요소와 데이터 흐름(data flow)을 나타내며 다음과 같은 10개의 주요 모듈로 구성된다.

상황정보 수집 모듈(Context Aggregator) u-City내 설치된 센서들이 감지한 정보를 수집하고, 사용자단말의 인증여부를 확인한다. 센서정보는 주로 사용자 개인단말과 그 단말 주변 센서 네트워크의 통신에 의해서 생성되고, 센서는 이 정보를 직접적으로 또는 상위 네트워크와의 통신을 통해



(그림 4) 프로파일기반 개인 정보보호 관리 아키텍쳐

간접적으로 상황정보 수집 모듈에 전달한다. 예를 들어, 개인 단말기를 소지한 사용자가 지하철역 안으로 들어서는 순간, 혹은 승용차를 타고 단지 입구를 빠져나가는 순간, 주변에 설치된 센서가 이를 감지하여 신호를 상황정보 수집 모듈에 송신하는 것이다. 수집된 센서정보 각각에는 센서가 감지한 시간 값(time stamp), 센서 일련번호(sensor ID), 사용자단말 식별정보와 인증정보, 사용자단말기의 사양(specification), 그리고 검사 합(checksum) 등이 포함된다.

인증정보는 센서가 감지한 사용자단말이 실제 사용자에 의해 인증된 단말인지 여부를 나타내는 정보이다. 이는 개인단말 분실 등의 이유로 타인의 단말을 통해 u-City 서비스를 이용함으로써 개인정보가 유출되는 것을 사전에 차단하기 위해 이용된다. 사용자는 로그인(log-in)이나 홍채 인식, 지문 인식 등의 방법으로 자신의 단말을 인증하게 되고, 인증이 이루어지지 않은 단말과 u-City내 센서의 통신에 의해 생성된 정보는 상황정보 수집 모듈에서 수신 후 사용자에게 단말기 인증을 요하는 메시지를 송신하고 인증완료 신호를 기다린다. 만일 일정 시간동안 인증이 이루어지지 않는다면 센서정보는 상황분석 엔진(Situation Analysis Engine)으로 전달된 후, 더 이상 상황추론과 서비스 제공 프로세스는 진행되지 않고 단말기 사용자 역시 u-City내에서 재난/재해 통보 서비스 등의 긴급서비스만을 제공받을 수 있다(guest mode).

상황분석 엔진(Situation Analysis Engine) 상황정보 수집 모듈로부터 전달받은 센서정보를 분석하여 현재 사용자에게 적합한 u-City서비스 목록을 출력한다. 센서정보에 포함된 시간 값, 센서 일련번호 등을 추출하여 데이터베이스(Knowledge Database)에 저장된 상황인지 온톨로지(ontology)

모델을 기반으로 현재 사용자의 상황을 추론하고, u-City 서비스 목록을 검색하여 현재 사용자에게 적절한 서비스 목록을 생성한다. 또 u-City 곳곳의 화재 및 재난 감시 센서에 의해 발생한 정보는 상황정보 수집 모듈을 거치지 않고 직접 상황분석 엔진으로 송신되는데 이는 개인단말별 분류, 인증확인, 센서정보 임시저장 등의 과정이 생략가능하고 인명구조, 위험통보 등의 긴급서비스를 보다 신속히 실행하기 위함이다.

보안정보 엔진(Security Information Engine) 상황분석 엔진으로부터 전달받은 서비스 목록을 데이터베이스에서 검색하여 해당하는 서비스 프로파일 목록으로 치환하는 엔진이다. (그림 4)의 정책적 명령은 임의로 변동되는 u-City 서비스 정책을 의미하며 제공이 일시 중단된 서비스, 또는 새롭게 추가되는 서비스 항목 등을 반영한다.

프로파일 비교기(Profile Comparison Module) 보안정보 엔진으로부터 전달받은 서비스 프로파일 목록과 사용자 단말로부터 수신한 사용자 프로파일을 각각의 서비스 항목별 프로파일 비교 동작을 한다. 프로파일 매칭이 이루어진 서비스 항목들은 출력되어 서비스구성 모듈(Service Configuration Module)로 전달되고, 매칭이 이루어지지 않은 경우 해당 서비스 제공 프로세스는 중지된다. 조건부 매칭이 이루어지는 경우에는 사용자 단말에 서비스 정보와 프로파일 설정 변경 메시지를 송신하고 사용자의 설정 변경을 기다리며, 또 화재/재해 통보 등 긴급 서비스의 경우에는 프로파일 비교 과정이 생략되어 사용자 프로파일 설정을 무시한 서비스 제공이 이루어진다.

데이터베이스(Knowledge Database) u-City에서 제공하는 모든 서비스의 프로파일, 상황추론과 맞춤형 서비스 검색을 위한 룰이나 상황 등의 정보를 저장하는 저장소로써 상황인지기반 지능적 서비스 제공을 위해 사용자 행동 패턴, 상황에 필요한 정보 등도 저장한다. 시스템 내 여러 모듈에 정보를 제공하고, 이는 데이터의 중복저장을 피함과 동시에 효율적인 업데이트를 가능케 한다.

서비스구성 모듈(Service Configuration Module) 사용자에게 제공될 맞춤형 서비스를 위해 서비스 컨트롤러(Service Controller)와 연동하여 실질적인 서비스 결정/실행을 지시하고 복잡한 충돌 문제 해소를 위해 각 서비스 단위를 통합관리할 수 있도록 하는 모듈이다. 또 사용자에게 서비스 제공시, 전달되는 정보의 보안을 유지하고 암호화 적용이 필요한 경우 보안 실행기(Security Behavior)에 명령한다.

정책반영 모듈(Policy Enforcement) 서비스별 보안정책과 여러 서비스 간의 우선순위를 정의하고 있으며 이에 따라 다양한 암호화 기법, 인증, 키 선택/분배 등의 보안정책이 각 서비스 실행 시 전달되는 개인정보의 분류 및 민감도에 따라 적절하게 실행될 수 있도록 한다.

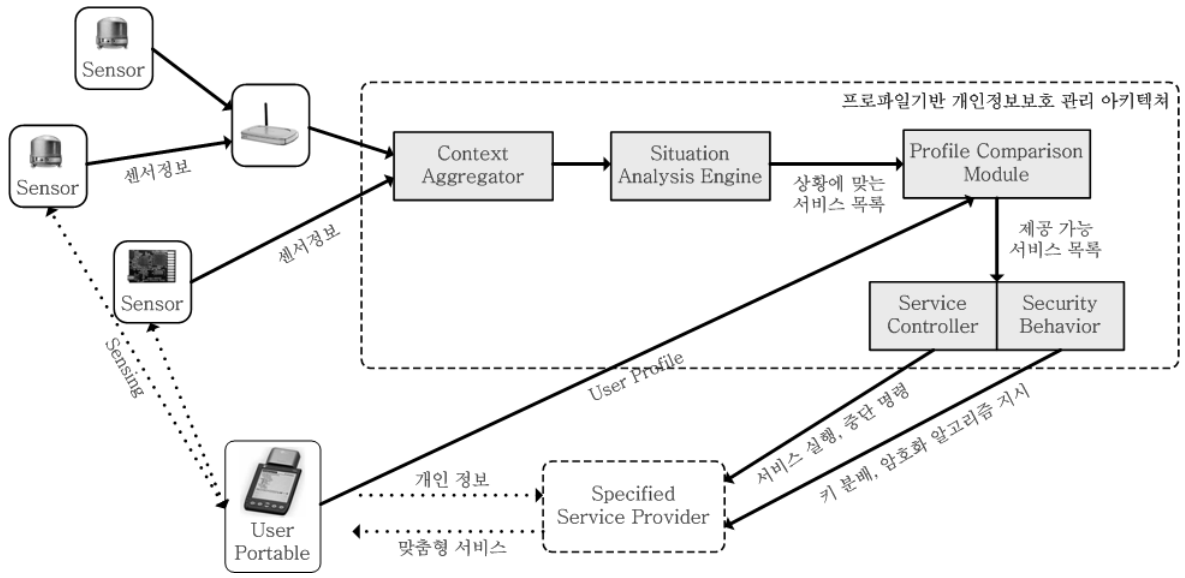
서비스 컨트롤러(Service Controller) 서비스 간의 충돌 발생을 방지하기 위한 서비스 스케쥴링을 수행함으로써 여러 서비스가 동시에 실행되어 충돌하는 것을 방지하는 역할을 한다. 서비스에 대한 데이터가 서비스구성 모듈로부터 전송될 경우, 먼저 서비스 분석을 수행한다. 서비스 분석이란 서비스의 등록 여부 및 서비스가 해당 위치에서 해당 사용자에게 제공될 수 있는지의 적절성 여부를 판단하게 되는 것을 뜻한다. 만일 해당 위치에서 우선순위가 높은 다른 서비스가 이미 수행중이거나 해당 사용자에게 권한이 주어지지 않은 서비스라면 이 단계에서 서비스 요청은 중단되고 사용자에게 제공할 수 없다는 메시지를 전송한다.

보안 실행기(Security Behavior) 사용자에게 제공될 해당 서비스에 대해 서비스구성 모듈로부터 명령이 전달되면, 해당 서비스 제공시 유통되는 개인정보의 분류 및 민감도에 따라 적절한 암호화 알고리즘과 키 시스템을 선택하여 출력한 후, 해당 서비스제공자(Specified Service Provider)에 전달한다.

보안 이벤트 모니터(Security Event Monitor) 사용자와 서비스의 상태 및 보안적용 상황을 저장하여 서비스를 시작할 경우 등록하고, 서비스가 종료될 경우 서비스의 최종 상태를 저장하여 다음에 서비스가 요청되면 동일한 보안 레벨을 적용케 하고, 최종 상태를 알려주어 서비스의 최종 상태에서부터 seamless한 서비스가 제공될 수 있도록 한다.

이와 같이 본 논문에서 제안하는 시스템은 사용자 프로파일과 서비스 프로파일의 매칭을 통해 u-City 맞춤형 서비스 환경에서 개인정보를 보호/관리하는 구조이다. (그림 5)는 제안하는 아키텍처의 주요 모듈(module)과 데이터 이동을 표시한 개략적인 흐름도이다. (그림 5)의 센서들은 u-City 곳곳에 위치하며, 사용자 단말기를 감지하여 그 센서정보를 직접적으로나 혹은 상위네트워크와의 통신을 통해 간접적으로 개인 정보보호 관리 아키텍쳐 안의 상황정보 수집 모듈에 전달한다. 예를 들어 개인단말기를 소지한 도시거주민이 아침 출근길 지하철역에 들어서는 순간, 또는 도시 내 박물관이나 공원입구에 들어서는 순간, 그 곳에 위치한 센서는 이를 감지하여 그 정보를 상황정보 수집 모듈로 송신하는 것이다.

이 후 상황정보 수집 모듈은 수집한 센서정보들을 각 사용자별로 상황분석 엔진에 전달한다. 상황분석 엔진에서는 데이터베이스에 저장된 상황인지 온톨로지 모델을 기반으로 전달받은 센서정보를 분석해 현재 사용자의 상황을 추론한다. 예를 들어 사용자가 버스 정류장에 들어선 순간, 감지된 센서정보를 상황정보 수집 모듈로부터 전달받았다면 상황분석 엔진은 센서가 감지한 시간 값과 감지한 센서의 위치 일련번호를 분석하여 가령 '현재 사용자는 아침 출근길이다.'라



(그림 5) 프로파일기반 개인 정보보호 관리 흐름도

는 상황을 추론한다.

또 상황분석 엔진은 추론한 사용자의 상황을 기반으로 현재 사용자에게 적합한 맞춤형 서비스 목록을 출력하는데 예를 들어, 대중교통을 이용하여 출근중인 위 사용자의 상황에 적절한 “맞춤형 전자신문 서비스”, “날씨/교통안내 서비스”등이 서비스 목록으로 출력되고, “화재/재난 응급통보 서비스” 같은 경우는 u-City 서비스 정책에 따라 사용자의 상황에 관계없이 기본서비스로써 출력될 수 있다.

프로파일 비교기는 사용자 단말로부터 사용자 프로파일을 수신하여 각 서비스 프로파일과 수신한 사용자 프로파일을 비교하고(compare process), 여기서 두 프로파일 간 매칭이 이루어진 서비스, 즉 현재 사용자에게 제공될 수 있는 서비스 항목들을 출력한다. (그림 5)의 서비스 컨트롤러와 보안 실행기는 u-City정책을 반영하여, 사용자에게 제공될 서비스에 대한 실행/중단 명령, 서비스 실행 시 전달되는 개인정보의 암호화 방법, 키 분배 등을 지시하는 파일(command file)을 생성하여 각각 해당 서비스 제공자(service provider)에게 송신한다. (그림 5)의 특정 서비스 제공자는 u-City 공공서비스를 위한 도시통합운영센터 내 서비스 제공 모듈(Service Provide Module)이거나, 혹은 외부에 위치한 상용/민간 서비스 제공 시스템이 될 수 있고 이러한 해당 서비스 제공 모듈은 서비스 컨트롤러와 보안 실행기에서 전달받은 파일(command file)을 반영하여 서비스 실행 시 전달되는 개인정보, 즉 현재 사용자의 위치, 직업, 스케줄 등의 정보를 안전하게 처리/보호 하면서 사용자에게 맞춤형 서비스를 제공한다.

command file의 주요 내용은, 사용자에게 맞춤형서비스가 제공될 때 오고가는 사용자 상황정보의 보호방법을 명령하는 것으로써 구체적으로는 서비스 제공시 유통되는 개인상황정보의 분류 및 레벨을 분석하여 암호화 알고리즘과 키 사이즈를 지시하는 것이다. 또한 이 command file을 수신한 서비스제공자 측에서는, 지시사항을 적용하여 사용자 단말과 통신을 하고 최종적으로 서비스제공이 이루어지는데, 이때 일반적으로 서비스제공자와 사용자 단말 사이에 공개키 기반의 키 분배가 먼저 이루어지고, 이 후 대칭키 암호화 기법을 사용하여 서비스 제공에 필요한 정보를 주고받게 된다. (그림 6)은 서비스 제공시, 유통되는 개인상황정보의 레벨에 따른 암호화 알고리즘과 키 사이즈 선택 테이블의 예시이다. 사용자에게 제공될 서비스에 대한 분석이 끝나면, 보안 실행기에서는 (그림 6)과 같은 테이블에서 적절한 암호화 알고리즘 및 키 사이즈를 선택하고, 기타 u-City보안 정책을 적용시켜 command file을 생성한다. (그림 6)에서 보여지는 바와 같이 네트워크를 통해서 전달되는 개인상황정보의 보안기법의 적용은 해당 정보에 대한 보안 강도, 정보의 크기, 디바이스의 컴퓨팅 파워에 따라서 상황에 따라 암호화 기법을 달리하게 한다. 이렇게 하는 것은 모바일 디바이스의 특성상 현재 배터리 상태를 비롯하여 컴퓨팅 능력이 일반 개인용 컴퓨터에 비해서 다소 떨어지기 때문에 상황에 다른 적절한 암호화 기법을 적용하여 보안성을 유지하면서 서비스의 편리성을 추구하는 장점이있다.

Security Level	Encryption algorithm/Key size	
Level 1	DES	56bit
Level 2	3-DES	56bit
Level 3	AES, SEED	128bit, 192bit, 256bit
Level 4	TBD	TBD

TBD : To be determined

(그림 6) 보안레벨에 따른 암호화 알고리즘과 키 사이즈 예시

2.6 테스트베드 구축 및 실험

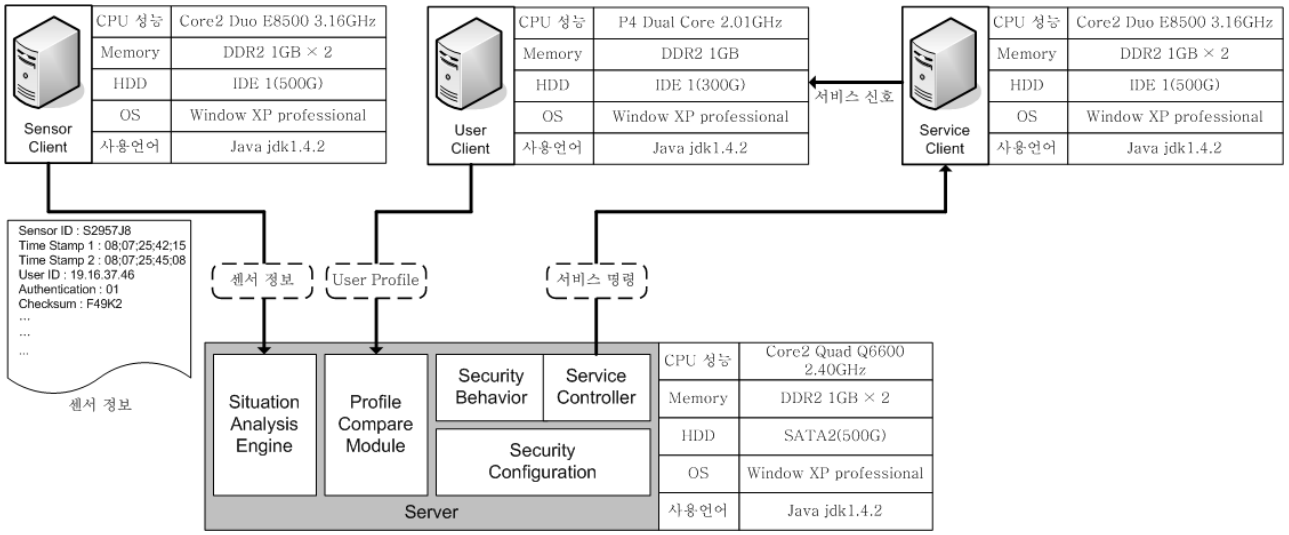
제안된 시스템의 성능을 측정하기 위해서 (그림 7)와 같이 테스트베드 환경을 구성하여 제안 시스템의 각 모듈의 처리 시간을 측정하였다. 테스트베드는 센서 클라이언트, 사용자 클라이언트, 서비스 클라이언트의 응용 프로그램을 사용하였다. 이때 사용된 하드웨어는 부분적으로 IDEC 지원을 받은 것이다. 센서 클라이언트는 u-City에서 센서역할을 담당하는 부분을 가상적으로 구현해 놓은 응용 프로그램이다. 이는 미리 정해진 센싱 정보를, 텍스트 형태의 메시지로 제안 시스템 서버로 전송한다. 사용자 클라이언트는 u-City구성원 역할을 담당하는 부분을 가상적으로 구현해 놓은 응용 프로그램이다. 이는 하나의 스레드당 한명의 사용자를 담당하고 사용자 프로파일을 전송하는 응용 프로그램이다. 서비스 클라이언트는 제안 시스템에서 프로파일 매칭을 통해 서비스 시작명령을 받으면 서비스를 가상적으로 실행하며, 서비스가 실행될 시 신호를 사용자 클라이언트로 보내 서비스가 제공되고 있다는 정보를 알려준다. 그리고 서버의 상황분석 엔진은 센서 클라이언트로부터 센서 정보를 입력받아 사용자 상황을 추론하고, 상황에 맞는 맞춤형서비스를 출력하는 역할을 하는데 이를 위한 온톨로지는 F-logic을 사용하여 구축하였으며, 이 온톨로지에 쿼리(query)를 해서 상황을 추론하고 서비스를 추출하는 과정은 SDOR(http://www.saltlux.com/)을 사용하여 구현하였다.

수행 시간 측정방법은 먼저 다중 사용자 클라이언트를 멀티스레드로 구현하고, 센서 클라이언트에서는 센싱 정보를 여러 번 전송하여 사용자 클라이언트에 서비스 실행 신호가 도착하기까지의 모듈별 평균 시간을 구하였다.

테스트베드에 적용된 u-City 서비스목록은 음성 길안내 서비스, 개인 스케쥴에 따른 업무 보조 서비스, 맞춤형 전자신문 서비스, 의료상담 서비스로 구성 하였다. 음성 길안내 서비스는 사용자의 목적지정보, 주변환경/날씨정보, 위치정보 등을 수신 받아 최단거리, 교통정체상황 등 다양한 정보를 제공해주는 것이고, 업무보조 서비스는 사용자의 스케쥴표를 읽어 들여 서비스를 제공한다. 맞춤형 전자신문 서비스는 사용자의 직업, 취미, 관심사 등을 분석하여 관련업계 동향이나 신제품 소식을 제공한다. 의료상담 서비스는 사용자의 체온, 맥박, 혈당 등의 신체상황정보와 의료 기록을 수신하여 주치의 상담을 받는 서비스이다.

(그림 7)은 본 시스템에서 모듈별 처리시간(processing delay)의 평균값과 서비스 컨트롤러를 기준으로 타 모듈의 처리시간 비율을 구한 것이다. 표에 따르면 업무 보조 서비스, 의료상담 서비스의 경우에는 보안 실행기의 처리시간이 500ms 이상이며 나머지 두 서비스에 비해 최소 160ms에서 350ms까지 처리시간이 더 긴 것을 볼 수 있고, 특히 의료상담 서비스의 경우에는 상황분석, 서비스 추론시간을 의미하는 상황분석 엔진의 처리시간이 544ms로 4가지 서비스 중 가장 길다. 또한 모듈별 처리시간 비율의 평균치를 보면, 프로파일 비교기와 서비스구성 모듈은 서비스 컨트롤러에 비해 각각 1.2배, 2.7배의 처리시간이 소요되며 이들 세 모듈은 전체 처리시간 중 차지하는 비중이 약 27.3%로 나타났다. 반면에 상황분석 엔진, 보안 실행기는 추론과정이 복잡하고, 정보 검색이 많아 전처리시간의 약 73.6%로 많은 비중을 차지하였다.

상황분석, 서비스 추론 시간을 나타내는 상황분석 엔진을 보면 의료상담, 업무 보조의 경우 사용자의 상황을 분석하고 적절한 서비스 추론에 필요한 센서정보가 많이 요구되고 시간, 공간, 과거 서비스 이용기록의 연관성에 따라 상황분석 결과 값이 다양하기 때문에 서비스 추론시간이 오래 걸린다. 또 보안 실행기의 처리 시간을 보면 의료 상담 서비스의 경우 722ms로 가장 많은 시간이 소요되었는데 이는 서비스 실행 시 전달되는 개인정보가 비교적 높은 보안레벨에 속해있고 따라서 복잡한 암호화 알고리즘과 큰 비트수의 키 값 선택에 의한 것이라 분석된다.



(그림 7) 테스트베드 환경

(단위 : millisecond)

	음성 길안내	업무 보조	맞춤형 전자신문	의료 상담	Average
Situation Analysis Engine	282	387	231	544	361.0
Profile Comparison Module	68	98	42	119	81.6
Service Configuration Module	136	219	101	281	184.3
Security Behavior	418	583	369	722	523.0
Service Controller	69	61	58	81	67.3
Total	973	1348	801	1747	

a. 모듈별 처리시간

	음성 길안내	업무 보조	맞춤형 전자신문	의료 상담	Average
Situation Analysis Engine	4.1	6.3	4.0	6.7	5.4
Profile Comparison Module	1.0	1.6	0.7	1.5	1.2
Service Configuration Module	2.0	3.6	1.7	3.5	2.7
Security Behavior	6.1	9.6	6.4	8.9	7.8
Service Controller	1.0	1.0	1.0	1.0	1.0

b. 서비스 컨트롤러(Service Controller)기준 타 모듈 처리시간 비

(그림 8) 프로파일기반 개인 정보보호 관리 시스템의 Processing Delay

3. 결 론

u-City환경에 기반한 개인 정보보호 관리 시스템을 구축하기 위해서는 먼저 서비스 제공에 이용되는 개인상황정보의 분류와 등급화가 필요하고, 다양한 상황정보와 u-City 각 서비스간의 연관성을 기반으로 사용자/서비스 프로파일을 표현하는 기술이 요구된다. 또한 곳곳의 센서들로부터 수집된 정보를 요약, 분석, 처리, 가공하여 이러한 정보를 기반으로 맞춤형 서비스를 제공하기 위한 상황인지 추론 시스템 구현이 선행되어야 한다.

본 논문에서는 u-City 맞춤형 서비스 환경에서 요구되는 다양한 개인의 상황정보를 개략적으로 분류, 등급화 하였고, 이를 기반으로 사용자 프로파일과 서비스 프로파일을 정의하여 프로파일 매칭을 통한 서비스 제공여부를 결정하고, 전달되는 개인정보의 암호화, 이를 위한 키 분배를 관리하는 정보보호 관리 구조를 제안하였다. 앞으로 u-City가 구현되고 서비스가 늘어나면 수집되는 센서정보가 다양해지고 이에 따라 해석해야 될 사용자의 상황이 증가할 것이다. 또 서비스 제공에 필요한 개인정보가 세분화됨에 따라 사용자/서비스 프로파일과 개인정보의 분류, 수준이 복잡해질 것으로 예상된다. 따라서 상황분석 온톨로지 모델에 관한 연구와 더불어 서비스 참여자들 상호간 협업을 통하여 개인정보의 수준별 세부분류 및 프로파일 표준화에 대한 연구가 지속되어야 할 것이다.

참 고 문 헌

[1] 전영옥, u-City의 성공적인 개발 모델과 시사점, 삼성경제연구소, 2006.

[2] 장희선, 김동철, 한성수, “u-City 주요 서비스 및 현안”, 한국디지털콘텐츠학회지, 제2권 제1호, pp.3-9, 2006.

[3] 박준홍, 고대식, “u-City 사업을 위한 고객 지향적 u-City 서비스 모델 개발에 관한 연구”, 한국정보기술학회 2007년도 하계학술발표논문집, pp.366-371, 2007.6.

[4] 장희선, 조기성, “송탄 u-City의 성공적인 비즈니스 모델”, 한국콘텐츠학회논문지, 제7권 제11호, pp.223-231, 2007.

[5] 권오병, 이남연, “장비협업도를 활용한 상황인식 시스템에 대한 구조적 평가 방법론”, 한국지능정보시스템학회논문지, 제13권 제2호, pp.27-41, 2007.6.

[6] 한국정보보호진흥원, 유비쿼터스 프라이버시 보호 종합대책 수립, 한국정보보호진흥원, 2006.9.

[7] 이준규, 이창훈, 김지호, 송오영, “U-City 환경에서의 개인정보 보호 향상을 위한 상황인지기반 보안 기법 연구”, 제29회 한국정보처리학회 춘계학술발표대회논문집, 제15권 제1호, pp.1132-1134, 2008.5.

이 준 규

e-mail : jg3546@wm.cau.ac.kr

2008년 중앙대학교 전자전기공학부(학사)

2008년～현 재 중앙대학교 전자전기공학부 석사과정

관심분야 : USN, 상황인지, 네트워크 보안, WLAN 및 WPAN 등

김 지 호

e-mail : jihokim@wm.cau.ac.kr

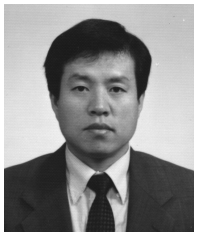
2000년 중앙대학교 전자전기공학부(학사)

2002년 중앙대학교 전자전기공학부(공학석사)

2007년 중앙대학교 전자전기공학부(공학박사)

2007년~현 재 중앙대학교 전자전기공학부 연구교수

관심분야 : 유비쿼터스 컴퓨팅, 상황인지, 네트워크 보안, WLAN 및 WPAN 등



송 오 영

e-mail : song@cau.ac.kr

1980년 서울대학교 전기공학과(학사)

1982년 한국과학기술원 전자전기공학과 (공학석사)

1992년 메사츄세츠 컴퓨터공학(공학박사)

1991년 10월~1992년 10월 Intergraph Corp 수석연구원

1992년~1993년 IBM Corp. 수석연구원

1994년 1월~1994년 8월 삼성전자 LSI 사업부 수석연구원

1994년 9월~현 재 중앙대학교 전자전기공학부 교수

관심분야 : Ubiquitous & Pervasive Computing, IMS, Mobile Computing, Wireless Network Security & Privacy 등