u-City 환경에서 공개키 기반 유아관리 시스템 설계

김갑열*, 박석천**
*경원대학교 소프트웨어학부
e-mail:scpark@kyungwon.ac.kr

Design of Public Key based Infant Management System in u-City Environment

Kap-Yol Kim*, Seok-Cheon Park**
*Division of Software, Kyungwon University.

요 약

최근 도시화 가속도로 가족단위가 축소되고 맞벌이 가정이 늘어나면서 육아문제가 대두되기 시작하였다. 이러한 문제는 도시를 살아가는 젊은 부부들의 저출산 문제를 야기하고 있으며 사회일각에서는 저출산 문제로 인한 미래 노동 생산력 우려를 거론하기도 한다. 따라서 본 논문에서는 이와 같은 문제를 해결하기 위한 방안으로 우리나라의 세계적인 IT 인프라와 정보통신 기술을 활용하고 유비쿼터스 사회 도래로 인한 u-City 구축을 위한 공개키 기반 유아관리 시스템 설계하였으며 이를 위해 Mobile RFID 기술과 ECC 기반 키 교환기법, 메시지 암호화 기법을 연구하였다.

I. 서론

과거 100년 전만 해도 사회를 구성하는 인구는 10% 가량만이 도시에 거주하고 있었다. 하지만 1980년 이후 산업의 발전으로 도시화가 가속되어 2050년 이후에는 전 세계 인구의 70%인 64억 명 가량이 도시에 거주할 것으로 예상되며[1] 이러한 도시화의 진행은 가족단위를 축소시키고 맞벌이 가정의 증가에 의한 육아 문제, 저 출산 문제, 환경오염 문제, 고령화 문제 등을 만들고 있어 도시민 생활 전반의 여유를 잃어 가고 있다. 특히 우리나라의 도시화 진행은 2020년 전국 대도시를 제외한 수도권의 인구 거주 예상 비율이 52% 달할 만큼 집중적으로 빠른 추세를 보이고 있어 그 문제의 심각성을 더하고 있으며[2] 이에 따라 도시생활을 편리하고 쾌적하게 할 수 있는 u-City에 대한 사람들의 관심이 증폭되고 있다. 따라서 정부는 이러한 도시민의 요구에 대응하기 위해 세계 최고의 IT 인프라와 정보통신기술을 활용한 u-City 시범 사업 연구를 활발히 진행하고 있으며 특히 도시민들의 생활과 직접 관련된 u-Home과 u-Healthcare의 연구 진척은 더욱더 빠른 추세를 보여 관련기술을 세계시장에 수출하고 있다. 그 예로 경기도 U-Healthcare RIS 사업단의 경우 인도네시아 국립심장병원과 현지법인 아린도사(PT.ARINDO)와 공동으로 인도네시아에 u-Healthcare 서비스 계약을 체결하였으며 경기중소기업종합지원센터는 말레이시아, 싱가포르, 인도네시아를 대상으로 수출상담회를 개최하여 성과를 얻기도 하였다[3].

본 논문에서는 이와 같이 세계 최고의 IT 인프라와 정보통신 기술력의 활용으로 도시화의 가속도에 의한 문제 중 맞벌이 가정의 증가에 따른 육아 문제에 대한 해결책을 제시한다. 이를 위해 유치원에서의 유아의 교육 상황과 영양 섭취 상황 등을 쉽게 파악할 수 있는 기능을 부모에게 제공하는 것을 목표로 u-city 환경에서의 공개키 기반의 유아관리 시스템을 설계하였다.

II. 관련 연구

2.1 u-City

유비쿼터스(Ubiquitious) 환경은 언제, 어디서, 어떤 매체를 통해서든지 모든 사물이 상호 통신할 수 있는 환경을 의미하며 이러한 유비쿼터스 환경에서는 사람과 사물이 상호 통신능력을 갖게 되고 네트워크로 연결되는 보다 확장된 미래 IT 환경이라 할 수 있다. 유비쿼터스 환경은 기술, 비즈니스, 의료 및 각종 사업 분야에서 다양한 서비스가 제공될 것이며 특히 기업경영, 유통 관리, 지식관리, 자산관리 등 비즈니스 분야에 많은 부가 가치를 창출 할 것으로 기대한다[4].

u-City는 유비쿼터스(Ubiquitious)와 도시(City)의 합성

* 경원대학교 일반대학원 전자계산학과 석사과정
** 경원대학교 IT대학 교수(교신저자)

어로 지능화된 첨단 도시를 의미하며 첨단 정보기술과 IT 기술발전을 기반으로 한 건설, 가전 및 문화와의 융합을 통한 블루오션(blue ocean) 신도시라 할 수 있다. u-City는 주민의 편의, 복지, 안전도를 높이고 이를 통해 신산업을 창출하는 등 경제적 효과와 더불어 근본적으로 주민의 삶의 질을 향상시키는데 목적을 두고 있으며 우리나라는 중앙 정부와 지자체 차원에서 u-City 활성화를 위한 사업을 활발히 진행하고 있다[5].

2.2 Mobile RFID

RFID는 무선주파수를 이용하여 사물에 부착된 태그(tag)의 IC칩에 저장되어 있는 고유 정보(data)를 안테나와 리더를 통해서 비접촉 방식으로 수집하여 대상물체를 판독 및 인식하는 기술로 유비쿼터스 컴퓨팅의 핵심 기술로 인식되고 있다[6].

Mobile RFID는 리더와 태그를 Mobile 단말(예, 휴대폰, DPA 등)에 내장하여 태그에서 취득한 정보나 내장된 태그의 정보를 이용하며 이동통신망을 통해 서비스를 받는 기술로서 기존 RFID와의 차이점은 이동통신망을 사용하고 태그와 리더를 한곳에 구성하는데 있다. 이동통신망의 사용은 여러 응용서비스와 직접적인 결합으로 인한 다양한 서비스를 창출할 수 있다는 점에서 기존 물류중심 서비스의 RFID 보다 큰 가치를 가지게 된다. 다음 그림 2.1은 Mobile RFID 네트워크 구조를 보여준다[7].

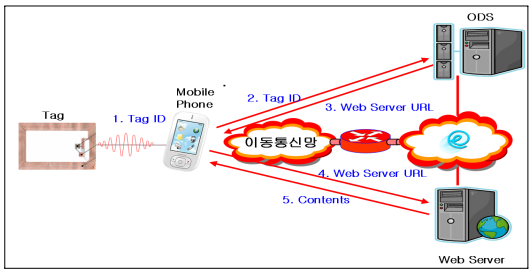

그림 2.1 Mobile RFID 네트워크 구조

일반적으로 유비쿼터스 환경에서의 RFID 시스템은 낮은 연산 능력, 제한된 메모리 용량 및 저 전력으로 사물과 사용자의 정보가 유통되는 과정에서 유출 가능성과 이로 인한 개인 정보 침해의 단점을 가지고 있으며 따라서 이를 해결하기 위한 연구는 향후 유비쿼터스 환경 구축을 위한 이슈가 되고 있다[8]. 특히 Mobile RFID 시스템의 경우 개인화에 따른 특수 목적의 서비스 모델을 지향하고 있어 이러한 정보 유출의 가능성은 기존 RFID 시스템보다 더욱 큰 문제로 인식될 수 있다. 따라서 본 논문에서는 공개키 기반의 암호 알고리즘을 적용한 유아 시스템을 설계하여 이에 대한 해결책을 제시하고자 한다.

2.3 ECC 알고리즘

ECC 알고리즘은 유한체 위에서 정의된 타원곡선 군에서 이산대수 문제의 어려움에 기초한 암호 시스템이다[9]. 본 논문에서는 유아 정보를 보호하기 위해 ECC 알고리즘 기반의 키 교환기법과 메시지 암호기법을 사용 하였다.

2.3.1 ECDH 알고리즘

본 논문에서 사용하는 암호 기법은 기본적으로 ECC 알고리즘을 이용한다. 하지만 이 기법을 사용하기 위해서는 난수와 결합한(예, P+P+P... = kP) 공개키를 송·수신 단말에 공유하여 공격자가 유추할 수 없는 비밀키를 동기할 수 있어야 한다. 이러한 문제를 해결하는 방법이 키 분배 알고리즘으로 1976년 W. Diffie와 M. E. Hellman에 의해 "New Directions in Cryptography"에서 제안되었고 이는 공개키 암호 알고리즘의 시초가 되었다. 향후 Diffie-Hellman의 키 분배 알고리즘은 여러 공개키 암호 알고리즘에 응용되었으며 ECC 알고리즘에서도 Diffie-Hellman의 키 분배 알고리즘을 이용한 ECDH(Elliptic Curve Diffie-Hellman)가 제안되었다.

ECDH는 유한체위의 Diffie-Hellman 알고리즘을 그대로 타원곡선위에서 변환한 것으로 본질적으로 Diffie-Hellman 알고리즘과 동작 방법이 같다[9]. 다음 그림 2.2는 ECDH 알고리즘의 동작 과정이다.

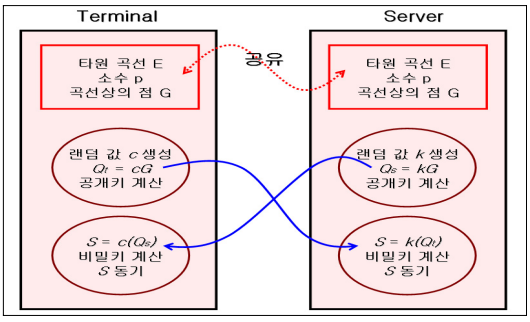

그림 2.2 ECDH 동작 과정

그림 2.2에서 최초 터미널과 서버는 타원곡선 E(E를 구성하는 파라미터 포함)와 곡선의 범위를 나타내는 p, 곡선상의 임의 점 G를 공유한다. 각 디바이스들은 랜덤 값 c, k를 생성하고 임의 점 G를 랜덤 값과 스칼라곱(G+G+G...)하여 공개키를 생성 교환한다. 교환한 공개키는 다시 자신의 랜덤 값과 스칼라곱하며 계산된 결과 값은 서로 같은 값을 가지는 비밀키 S가 된다. 이와 같은 방법으로 동기된 S는 서명을 위한 도구나 메시지를 암호화하는 암호키로 이용할 수 있고 메시지를 암호화하는 방법으로는 EC-ElGamal이 대표적이다.

2.3.2 EC-ElGamal 알고리즘

EC-ElGamal 알고리즘은 Diffie-Hellman의 키 분배 알고리즘을 바탕으로 메시지를 암호화 하는 방법으로 현재 ECC 알고리즘 기반의 암호 기법 중 가장 많이 사용하는

암호 알고리즘이다[10]. 다음 그림 2.3은 EC-ElGamal 알고리즘 동작을 나타내며 비밀키(S)를 계산 해내는 과정은 Diffie-Hellman의 키 분배 알고리즘과 같다.

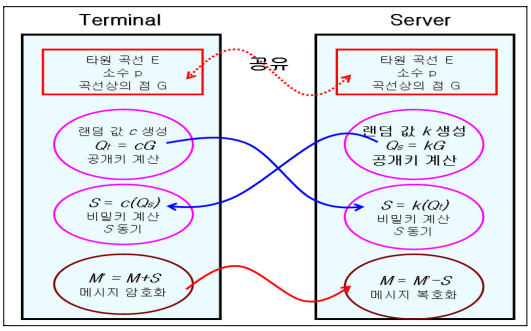

그림 2.3 EC-ElGamal 동작 과정

EC-ElGamal의 메시지 암·복호는 비밀키 계산 이후 터미널이 메시지(M)와 비밀키를 플러스 연산(암호)하여 서버에 송신하는 과정과 서버가 암호화된 메시지(M′)를 비밀키를 이용 마이너스 연산(복호)하는 과정으로 나타낸다.

III. 공개키 기반 유아관리 시스템 설계

3.1 시스템 구성

본 논문에서 제안하는 유아관리 시스템은 도시화 가속도에 의한 맞벌이 부부를 위해 저학년 자녀 관리를 효율적으로 할 수 있도록 하는 시스템이다. 본 시스템은 모바일 RFID 시스템의 응용으로 정보의 대상자가 되는 자녀에게는 목걸이형 RFID 태그를 발급하고 정보를 제공받는 주체가 되는 부모 또는 경찰과 정보 제공 주체인 교사는 모바일형 RFID 리더를 가지고 있어야한다. 본 시스템은 기본적으로 자녀 개인의 정보를 다루고 유아의 생활 패턴이나 생활환경 수준 등을 유추할 수 있는 정보를 송·수신하며 이 같은 정보로 범죄 또는 프라이버시 침해에 이용할 수 있으므로 데이터 보호를 위한 보안 기법이 필수적으로 강구되어야 한다.

본 시스템은 효율적인 설계를 위해 시스템의 동작 목적과 성격에 맞게 다음 표 3.1과 같이 나눌 수 있다.

표 3.1 제안 시스템 구분

구분	설명
RFID Tag	1. 유아를 인식할 수 있는 시리얼 데이터를 Reader에 송신
RFID Reader (미들웨어)	1. Tag의 데이터를 읽음 2. 해당 콘텐츠 서버 또는 ODS 서버에 접속하여 데이터 송·수신
통합 Server	1. Tag 데이터에 해당하는 정보를 가짐 2. 인가된 정보 요청자에 데이터 송신 3. 인가된 관리자에 의한 정보를 수신·저장
ODS Server	1. Tag 데이터에 해당하는 콘텐츠 서버 주소를 송신함

표 3.1에 구분된 시스템은 모바일 단말을 이용한 특징으로 무선 인터넷 또는 이동 통신망을 통해 연동 된다. RFID 미들웨어와 통합 Server 구간의 정보 송·수신시에는 Tag의 시리얼 데이터를 전송하며 무선 통신 환경으로 인한 정보 유출의 가능성이 크게 되므로 공격자로부터 데이터를 보호할 수 있는 ECC 알고리즘을 적용한다. 다음 표 3.2는 제안 시스템의 구현환경을 보여 준다.

표 3.2. 제안 시스템 구현 환경

구성 요소		사 양
통합 서버 • ODS 서버	CPU	Intel Duo Core 2.66Ghz
	RAM	2GB
	이더넷 카드	Realtek RTL-8168
	운영체제	Windows XP pro
	개발 플랫폼	Visual Studio 2005(C#)
미들웨어	CPU	Intel Core2 2.00Ghz
	RAM	512MB
	이더넷 카드	Intel PRO 3945ABG
	운영체제	Winddows CE core 5.0
	개발 플랫폼	Visual Studio 2005 Pocket PC 2003 SDK(C#)
Tag/Reader	System	ER200 Development kit

3.2 시스템 설계

다음 그림 3.1은 본 논문에서 제안하는 u-City환경에서 공개키 기반 유아관리 시스템의 개요도이다.

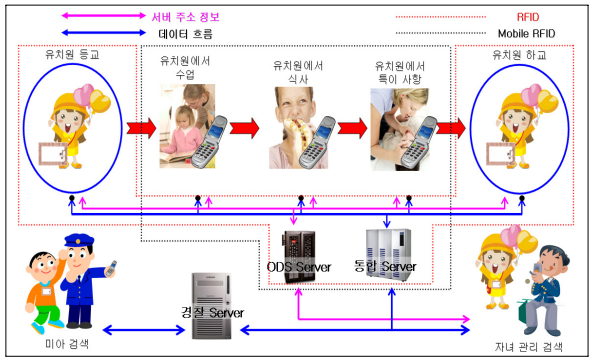

그림 3.1 제안 유아 관리 시스템

그림 3.1에서 유치원 교사는 태그를 부착한 유아의 정보를 모바일 단말로 인식하여 ODS 서버로부터 해당 콘텐츠를 제공하는 Server URL을 받는다. 이후 관리자 로그인을 통해 해당 유아의 정보를 입력할 수 있는 콘텐츠를 제공받아 당일 받았던 교육 내용과 급식, 발육 상태 또는 특이사항 등을 기록한다.

부모가 가진 모바일 단말의 역시 유치원에서 돌아온 유아의 태그 데이터를 읽은 후 ODS 서버로부터 Server URL을 받고 해당 콘텐츠 서버에 접속하여 당일 자녀에 대한 사항 등을 조회하여 자녀의 교육 및 발육 상태 등을 체크할 수 있다. 또한 본 시스템은 경찰 서버와 연계하여 태그를 부착한 유아가 길을 잃어 미아가 된 경우 미아의 정보를 검색할 수 있도록 하여 미아 찾기 시스템으로도

활용할 수 있다. 다음 그림 3.2는 제안하는 시스템에서 태그인식과 데이터를 조회하는 절차를 보여 준다.

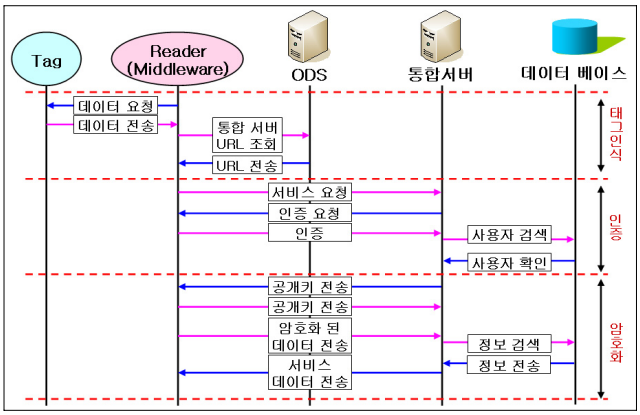

그림 3.2 서비스 절차 예

그림 3.2와 같이 서비스 절차는 크게 3부분으로 나눌 수 있으며 인증부터 암호화 절차는 최초 1회만 실행된다. 만약 사용자가 로그아웃을 요청하거나 일정시간 서비스 요청이 없을 시에는 인증이 자동 해지되며 사용자가 서비스 재요청시에는 다시 인증과 암호화 절차가 실행되어야 한다. 이때 사용자 편의를 위해 인증을 위한 ID와 Password는 선택적으로 고정할 수 있도록 하며 암호화 절차 이후부터 모든 서비스 송·수신은 동기된 비밀키를 이용하여 데이터가 암호화되므로 이를 처리할 수 있는 모듈도 구현되어야 한다. 다음 그림 3.3은 암호화 이후 통합서버에서 데이터 처리를 위한 동작흐름을 나타낸 것이다.

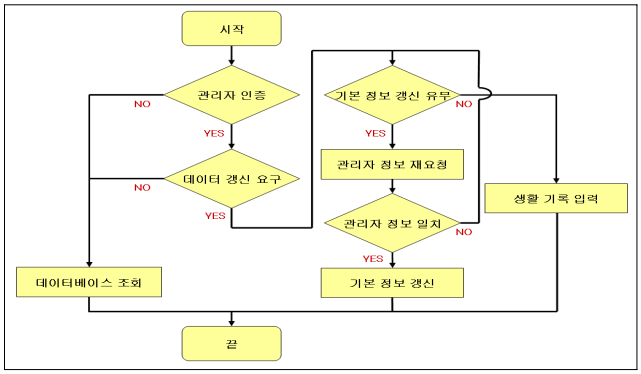

그림 3.3 데이터 처리 동작

그림 3.3에서 통합서버는 단순 사용자와 유아의 정보를 갱신할 수 있는 권한을 가진 관리자를 구분하여 서비스 종류를 처리할 수 있어야 한다. 따라서 관리자 인증 확인 후 관리자가 아닌 경우 단순 유아 정보만 조회하도록 하며 관리자인 경우 유아 개인정보까지 수정할 것인가 아니면 그날의 생활기록만 수정할 것인가를 구분하여 서비스 할 수 있는 메뉴를 구성한다. 만약 관리자가 유아 개인정보를 수정할 경우 인증을 재차 요구하여 혹시 있을 문제에 대비할 수 있도록 한다.

IV. 결론

본 논문에서 제안하는 유아관리 시스템은 유비쿼터스 컴퓨팅 핵심기술 중 자동 사물식별기술인 RFID 시스템을 활용하여 구성하였다. 특히 이동성을 최적화하고 실시간으로 유아의 정보를 확인할 수 있도록 특화된 Mobile RFID 기술을 적용하여 효율성을 극대화 하였으며 Mobile RFID의 보안상 취약점을 해결하기 위해 ECC 알고리즘 기반의 ECDH 키 교환기법과 EC-ElGamal 메시지 암호기법을 적용하여 설계하였다.

본 시스템은 도시화에 의한 맞벌이 가정의 증가에 따른 육아 문제에 대한 해결책으로 제시하였으며 특히 유치원 이하 저 연령 자녀와 의사소통을 원활히 할 수 없는 유아를 둔 가정에서는 자녀의 성장상태, 교육상태, 기타 문제 등을 쉽게 파악할 수 있어 u-City 사회를 살아가는 젊은 층 부모의 유아관리에 대한 요구를 쉽게 해결할 수 있을 것이라 생각한다. 또한 본 시스템이 적용된 태그를 부착한 아이가 길을 잃게 될 경우 경찰 정보 시스템과 연동하여 쉽게 미아의 개인정보를 확인할 수 있게 하고 이를 통해 미아 찾기 시스템으로 활용할 수 있을 것이라 기대된다.

참고문헌

[1] 구정은, “연내 전세계 인구 절반이 도시인”, 문화일보, 2008.02.27.

[2] 강철원, “도시화 과정 및 발전방향”, 경기도 도시계획과, 2006.07.14.

[3] http://www.kyungwon.ac.kr

[4] 오수현 외 “유비쿼터스 환경에 적합한 사용자 프라이버시 보호 기능을 제공하는 RFID 시스템”, 한국통신학회논문지, pp.1729-1738, 2004.

[5] 조병선 외 “미래 최첨단 신 도시 u-City에 미리 가볼까”, ETRI CEO Information 제44호, 2006.10.30.

[6] 김원, 나정정, “RFID 검색시스템 구축 및 운영 지침서 V1.2”, NIDA.KO, Dec, 2006.

[7] 김형준, “표준기술동향: 모바일 RFID”, TTA Journal No. 99, 2005.05.

[8] Miyako Ohkubo et al, "Cryptographic Approach to 'Privacy-Friendly' Tags," RFID Privacy Workshop, 15. Nov. 2003.

[9] SEC1, “Elliptic Curve Cryptography,” v.1.0, pp.62, Sept. 2000.

[10] O. Ugus et al, "Performance of Additive Homomorphic EC-ELGamal Encryption for TinyPEDS," Technischer Bericht der RWTH Aachen ISSN 0935-3232, Germany, July, 2007.