디지털산업정보학회 논문지 제6권 제2호-2010년 6월

유비쿼터스 RFID 개인정보 침해에 대한 방안 연구

최 희 식* · 박 재 표** · 전 문 석***

A plan research about a Ubiquitous RFID infringe private information

Choi, Hee Sik · Park, Jae Pyo · Jun, Mun Seog

〈Abstract〉

RFID System of Ubiquitous which is one of problem that may occur in a process of replacing bar code in 21st century. Ubiquitous computer environment should be considered to be most important task to protect information.

For introduction, this presentation going to discuss the background information, the purpose of Ubiquitous and potential problems in individual privacy in computer environment.

In main part, the content will handle the practices and weakness in security of computer environment in Ubiquitous. Last part of presentation going to examine, futuristic views in solving existing problems with alternative solutions to prohibit invasion in privacy.

Key Words : RFID(Radio Frequency Identification), Private Infringement, Data Protection

Ⅰ. 서론

정보통신의 발달로 사회 전반적인 구조가 정보 사회로의 진입하여 사회 구조 역시 빠르게 정보 변화에 대한 물결이 거세게 일고 있다. 국내에서도 정보환경 변화에 따른 유비쿼터스 RFID 기반 환경의 도입이 늘고 있는 추세에 따른 RFID/USN(Radio Frequency IDentification/ Ubiquitous Sensor Network) 비접촉 센서의 사용증가로 인한 사회에 미치는 개인 정보 침해에 대한 부정적인 부분이 사회의 문제점으로 이슈화 되고 있다[3-4].

RFID는 원래 기존의 바코드를 대체할 새로운 수단으로 사물에 태그(Tag)를 부착하여 정보를 실시간으로 탐지하여 각종 물품관리, 재고관리, 물류관리, 동물관리 등에 사용하여 이용자에게는 편리성과 관리자에게는 필요한 관리적인 측면에서 필요한 정보를 제공하는 것이다[2].

이렇게 편리하게 사용하고 있는 RFID 태그 정보는 개인의 프라이버시 침해를 제공하는 위험적인 요소를 지니고 있다. 예를 들어 한 리더기가 제품에 대한 정보를 읽어 들이게 되면 주변의 일정한 반경 내의 리더기 들은 태그 정보를 입력받게 된다.

예를 들어 한 고객이 백화점에서 물건을 구입하게 되

* 숭실대학교 일반대학원 컴퓨터학과 박사과정(제1저자)
** 숭실대학교 컴퓨터학과 교수(교신저자)
*** 숭실대학교 컴퓨터학과 교수

면 어떤 제조사의 옷을 샀는지, 가격은 얼마인지, 색상은 어떤 색인지, 사이즈는 얼마인지, 어떤 백화점에서 물건을 선택했는지에 대한 정보가 노출되게 된다. 개인의 신상과 프라이버시적인 정보가 외부로 노출되게 되고 또 다른 불법적인 상업 수단으로 제공된다면 자신의 위치적 정보 추적을 제공할 수 있게 된다.

본 논문에서는 2장에서는 유비쿼터스 시스템에 대해서 살펴보고 3장에서는 개인정보에 대한 내용으로 RFID를 통해 저장된 태그에 중요한 개인 정보가 어떻게 수집되어 잘못 전달되고 있으며, 읽혀진 정보가 어떠한 컴퓨터 시스템에 연결되어 불법으로 사용되고 있는지 살펴보았고, 4장에서는 RFID 무선 식별장치를 통해 우려될 수 있는 위험적 요소와 개인적인 침해 사실에 대한 피해 사례를 연도별, 유형별 통계 자료를 통해 분석하였으며, 5장에서는 개인침해에 대한 문제점이 시사 한 내용을 기반으로 어떻게 대처해야 하는지에 대한 해결책에 대해 살펴보았으며, 6장에서는 RFID 보안 기술 비교 분석, 7장에서 본 논문으로 인한 기대효과로 결론을 맺고자 한다.

Ⅱ. 유비쿼터스

유비쿼터스(Ubiquitous)란 다양한 종류의 컴퓨터가 사람, 사물, 환경 속으로 스며들고 서로 연결되어, 언제 어디서나 컴퓨팅을 구현할 수 있는 환경이다.

따라서 유비쿼터스 컴퓨팅은 이용자가 공기나 물처럼 의식하지 못할 정도로 일상생활 안에 스며들어 무의식적인 존재로 편리하게 생활할 수 있도록 되어야 한다. 이에 RFID라는 태그를 각 사물 등에 부착시켜 개인의 정보를 Reader기가 읽음으로써 사용자의 정보를 제공받고 사용자는 제공되는 편리성을 쉽게 이용하는 그런 시스템 인 것이다[5].

현재 RFID 시스템은 다양한 산업체 현장 및 소비자 제품 및 소비자 편리 시설에 사용되고 있으며, 주로 사용되고 있는 용도에는 접근 제어, 고객관리, 물류관리, 자재 관리, 창고 자동화 등이 있다[11].

<그림 1> 각종 RFID

Ⅲ. 개인정보

개인정보와 관련해 수많은 논의에서는 개인정보의 개념을 프라이버시라는 의미로 전달하고 있으며, 프라이버시는 대체적으로 서양에서 발전된 개념이다.

프라이버시 개념은 아주 오래전부터 시대나 역사 혹은 그 사회적인 조건에 따라 다양하게 정의되어 왔다. 초기의 프라이버시 개념은 'the right to be alone'의 뜻으로 개인적 삶의 영역에서의 최소한의 방어적 의미로 해석되었던 반면 최근에는 자신의 정보에 대한 통제권을 보장하는 정보 프라이버시(Information Privacy)의 개념으로 폭넓게 확장되어 사용되어 지고 있다.

따라서 최근에 문제시 되고 있는 개인적인 정보수집이 본인의 의도와는 전혀 다르게 수집되어지는 경우가 빈번함에 따라 앞으로 프라이버시 보호의 개념은 단순한 방어 차원에서 개인이 원하지 않는 한 철저하게 차단되고 보호되어야 하는 측면으로 법적인 근거 자료가 제시되어야 한다[9-10].

3.1 프라이버시와 개인정보의 의미적 차이

개인 정보보호의 정의에 앞서 프라이버시와 개인정보

의 차이점에 대해서 먼저 언급하고자 한다. 개인정보 보호 가이드라인('RFID 프라이버시 보호 가이드라인 해설서'(2007. 9. 18 발표)가 발표되면서 프라이버시와 개인정보를 혼동할 수 있는 경향이 있으므로 이러한 용어에 대해서는 주의 깊은 이해가 필요하다[12].

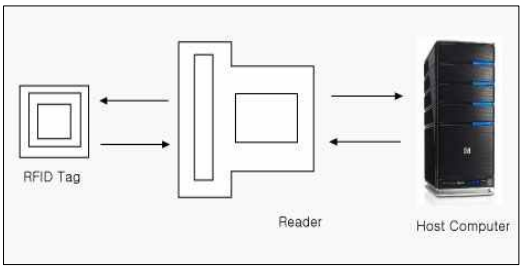
최근에는 컴퓨터를 통해 개인정보를 관리함으로써 개인정보에 관한 문제가 더욱 중요하게 받아들여졌다. 특히 이 부문과 관련된 프라이버시 문제를 정보 프라이버시라고 하였는데 정보 프라이버시(Information Privacy)는 개개인 자신 및 자신이 소속된 그룹과 관련된 정보를 통제할 수 있는 권리로 개인정보의 수집, 이용 유포와 관련된 의미성을 지니고 있다[6].

개인정보는 생존하는 개인 신상에 대한 정보로서 이름, 주소, 주민등록번호, 전화번호, 통장 계좌번호, e-Mail 등이 포함된 정보로 한 개인을 식별할 수 있는 수단을 제공할 수 있으며, 부호문자, 음성, 음향 및 영상 등의 정보와 더불어 개인의 신체, 재산, 사회적 직위, 신분 등에 관한 사실, 판단, 평가 등을 나타내는 일체 자료의 정보를 말한다. 그러므로 본 연구의 개인정보의 의미는 정보 프라이버시에 더욱 큰 비중을 두고자 한다. 개인 정보는 과거의 단순한 신분 정보에서 오늘날에는 전자상거래, 고객관리, 금융거래 등 사회의 구성, 유지, 발전을 위한 필수적 기능을 가진 요소로써, 기업의 입장에서는 고객의 개인정보가 수익 창출을 위한 재산적 가치로서 높게 평가되어지고 있다[8].

Ⅳ. RFID

4.1 RFID 시스템의 구성

RFID 시스템은 크게 안테나가 포함된 Reader기, 무선자원을 송·수신할 수 있는 안테나, 정보를 저장하고 데이터를 교환하는 Tag, Host Computer 등으로 구성된다[6].



<그림 2> RFID 시스템 구성도

■ 태그(Tag)

데이터를 저장하기 위한 하나의 마이크로 칩과 RFID 통신으로 데이터를 전달하기 위한 Coiled Antenna와 같은 하나의 Coupling Element로 구성된다. 사용전력, 마이크로칩의 포함 유무, 사용주파수 등에 따라 다양한 종류로 구별된다[6].

■ 리더기(Reader)

Reader는 신호를 보내고 받기 위한 안테나가 있으며 데이터를 디코딩하기 위한 transceiver와 processor로 구성된다. Reader는 휴대 가능한 단말기의 형태와 톨게이트 입구에서 통행료를 징수하는 고정 장치 형이 있다[6].

■ 호스트 컴퓨터(Host Computer)

Reader로부터 정보를 수집, 정리 및 처리하고 가공된 정보를 네트워크 또는 외부 시스템으로 전송한다[6].

4.2 바코드 시스템과 RFID 시스템 차이

아래 <표 1>과 같이 바코드 시스템에서는 단순히 개인의 직접적인 신상정보 또는 부가정보가 정보로서의 역할만을 하였고, RFID 시스템에서는 원칙적으로 물품자체에 대한 정보를 RFID가 기록 보유하고 있기 때문에 정보의 프라이버시적인 요소는 원칙적으로는 가지고 있지 않다.

<표 1> 바코드 시스템과 RFID 시스템의 차이

구분	바코드 시스템	RFID 시스템
특징	개인의 신상정보, 또는 부가정보	원칙적으로 개인정보가 아닌 물품자체에 대한 정보
	정보주체가 정보생성에 대해 인식을 하고 동의	정보수집 상황을 인식하기가 어려움

<표 2> RFID 태그정보 [15]

활용단계	단계별 형태	규제내용
RFID 생산	RFID 태그 생산	- RFID 관련 기술 표준에 맞추어 생산 - 개인 정보와 관련하여 규제할 필요 없음
RFID 태그에 정보기록	■ 물품 정보 기록 - RFID 생산자가 RFID 태그 구매자의 요청에 따라 관련 물품 정보를 기록 ■ 개인 정보 기록 - RFID 생산자가 RFID 태그를 정보가 기록되지 않은 상태로 판매하면, 사용자가 직접 개인정보 기록	- CODE 표준에 맞추어 물품정보를 기록 - 개인정보와 관련하여 규제할 필요 없음 - RFID 태그에 개인정보 기록을 제한(제4조) - 법률규정 또는 정보주체의 명시적 동의 없는 개인정보 기록을 금지 - 동의 획득 시 기록목적 등을 미리 정보 주체에 고지
RFID 부착	물품 생산자가 물품에 RFID 태그 부착	- RFID 태그 부찰 사실 등을 이용자가 용이하게 알아볼 수 있도록 설명하거나 표시(제7조) - RFID 태그 기능을 제거할 수 있는 방법을 설명하거나 표시(제8조)

4.3 RFID 태그정보 및 개인 정보 수집

개인정보 수집은 정부 기관에서만이 수집 및 관리를 하는 형태는 아니다. 정보통신기술의 발달로 민간사업자 즉 판매기업 등에서도 개인정보에 대한 수집 관리 및 이용이 매우 쉬워졌다. 국가나 민간사업자의 입장에서는 개인정보는 경제적 측면에서 대중을 통제하는 방법으로 또는 마케팅의 방법으로 활용하고 정보주체인 개인은 평등한 서비스를 즐길 수 있다는 측면에서 그 가치를 얻고 있다.

하지만 개인의 인격성의 보호라는 프라이버시 보호의 차원에서 계속 프라이버시권의 보호를 받을 수 있지만 <표 2>에서처럼 RFID를 통한 공동체 시스템 운영상 규제할 여의치 않는 부분에 대해서는 일정한 개인정보의 수집을 인정해 주는 것이 바람직할 수 있다. 이러한 권리는 단순히 사생활 보호의 측면으로만 바라보면 안 되고 정보 활용 권을 가진 정치적 사회적인 통제와 감시 권으로 인식될 필요성 측면에서 볼 때 역할 적으로 매우 중요하다 하겠다[13].

V. 개인침해 사례적 문제점 분석

5.1 불법 Reader기를 통한 데이터 수집

불법 Reader기들은 사용자의 허락 없이 읽혀진 태그 정보에 의해 데이터를 불법으로 입수하여 전송하는 형태이다. 그러나 일반적인 시스템에서는 상대방의 정보를 얻기 위해서 시스템 서버상에서도 인증 정보를 저장하여 유지 해야만 한다. Reader기의 인증을 확인하는 것이 일반적이지만 여기에서는 서버의 저장된 데이터를 활용하고 있는 경우이다.

5.2 Reader기의 보안 취약 문제점

태그는 Reader기에 데이터를 보내고 데이터의 전송을 완료할 때까지 메모리에 정보를 저장하고 부여된 기능을 실행하기 위해 데이터를 사용한다. 하지만 이러한 과정에서 Reader기는 보안의 취약성을 보이게 된다. RFID 는 유비쿼터스 환경 기반에 매우 중요한 기술로써 Reader기와 로컬서버의 커뮤니케이션을 무선으로 하게 된다. 유비쿼터스 환경에서의 대부분 Reader기는 Handheld Reader 로서의 역할을 하는 기기를 사용하게 되는데 이

러한 Reader기들은 이동성을 보장하기 위하여 무선 환경에서 로컬서버와 연결을 진행하게 된다.

RFID Reader기는 이러한 무선랜 환경에서 무선채널 전파를 사용하게 되는데 무선통신을 사용하는 과정에서 RFID Reader를 통해서 읽혀진 태그 안에 데이터가 보안상 취약점 <표 3>을 드러나게 하는 원인인 것이다.

<표 3> 숨겨진 태그의 보안 취약점[14]

구분	설 명
숨겨진 태그	RFID 태그들이 소유주인 정보주체가 인지하지 못한 상황에서 사물들과 문서에 내장 될 수 있다. 무선전파는 섬유, 플라스틱, 다른 물질들을 쉽게 통과할 수 있기 때문에 지갑, 쇼핑 백, 옷가방 등에 들어있는 사물 또는 옷에 부착된 RFID 태그 등이 읽혀지게 된다.
유일한 식별자	바코드와는 달리 RFID는 유일한 고유 ID를 가지게 된다. 유일한 ID번호를 가지게 됨으로써 사용되어진 ID는 판매된 시점 또는 이전 시점에서 신원이 파악되어 정보가 노출되게 된다.

5.2.1 RFID 구성 요소에 대한 보안 취약성 분석

RFID 시스템 구성 요소인 태그와 Reader기, 서버와 호스트컴퓨터 사이에서 요소마다 보안성에 취약성을 가지고는 있다. 특히 태그와 Reader기 사이, Reader기와 서버사이의 일반적인 무선랜 환경의 커뮤니케이션 문제성과, 불법적인 Reader에 의한 정보 유출과, 유출된 자료들이 제 3의 민간통신업자 시스템등과 연계되어 자료가 제공되는 취약적인 보안의 문제점들이 드러나고 있다.

뿐만 아니라 서버 내에서도 컴퓨터 해킹 등에 대한 관리 소홀, 관리자의 무심한 대처 미비로 인한 보안의 심각한 안정성이 매우 저조한 것으로 분석되었다.

5.2.2 연도별 개인 침해 현황 분석

본 연구를 통해 연도별 개인침해 피해 건수 <표 4> <그림3>가 연도별로 해마다 증가되고 있는 심각한 실태를 확인할 수 있다.

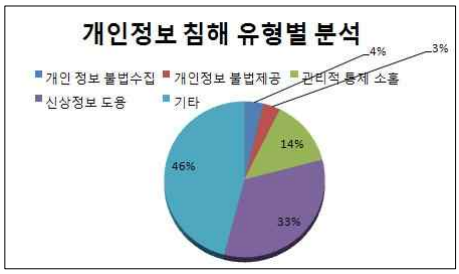
<표 4> 연도별 침해 발생 건수[14]

년도	2003년	2004년	2005년	2006년	2007년	2008년	2009년
개인침해 건수	17,777	17,569	18,206	23,333	25,965	39,811	35,167

<그림 3> 개인 정보 침해건수[14]

5.2.3 유형별 개인 침해 분석

RFID 태그 개인 정보 영역은 사용자의 이력 정보와 실시간 정보를 포함하고 있으며 특히 인증 확인 시 권한을 태그 데이터가 가지고 있는 경우에 심각한 위조 변조가 일어나고 있었다. 이 처럼 관리적 통제 소홀로 인해 태그 정보를 불법 사용자가 수정 또는 삭제하는 경우에 개인 정보 침해가 제 3의 정보제공업자에게 변형되어 아래 그림과 같이 유형별 분석 자료를 나타내고 있다.<그림 4>



<그림 4> 개인침해 유형별 분석[14]

5.3 RFID의 문제점 대응 방안 연구

RFID 기술은 유비쿼터스 환경에서 핵심적인 중요한 기술이지만 개인정보 침해 가능성이라는 큰 문제점을 가지고 있는 것은 사실이다. 여기에서 이 문제점을 좀 더 세분화하여 정보를 수집하거나 제공할 때 <표 5> 유형별 개임침해 자료를 통해 확인한 바와 같이 정보가 제공되어 타 시스템 정보와 결합되어 진 경우, 정보가 관리되는 시점에서 사용자의 위치적 정보가 읽혀진 경우의 문제점을 시사해 보자.

<표 5> 유형별 개인 침해 [14]

침해 유형	건수	백분율
개인 정보 불법수집	165	4%
개인정보 불법제공	146	3%
관리적 통제 소홀	590	14%
신상정보 도용	1,430	33%
기타	1,974	46%

5.3.1 정보 수집 측면 해결 방안에 대한 연구

RFID는 특성상 확인 및 시스템의 인식이 타 시스템 및 다른 기술이나 방법에 비해 어렵기 때문에 개인정보와 프라이버시 보호에서 보다 적극적인 보호조치를 취해야 한다. 정보주체는 RFID Reader의 수집되는 내용 등에 대해서도 충분히 인지해야 할 권리가 있으며, 원하지 않는 정보 수집에 대해서는 Reader기의 Access를 차단하여 원하지 않는 정보가 차단되어야 한다.

그리고 이를 시행치 않을 경우에는 법적인 강력한 대응 조치가 반드시 마련되어야한다.

그것은 RFID를 이용하는 이용자의 권익과 사업자의 권익도 보호돼야 할 필요성이 있기 때문이다. 만약, 포괄적 동의의 경우에는 일반적으로 세부적인 내용에 대한 인식이 불가능한 경우가 발생할 수 있으며, 이는 정보주체에게 불이익을 제공하는 경우가 발생할 수 있기 때문에, 개인정보 주체의 동의 철회 절차를 비교적 간소화시켜 개인 정보 주체의 권익을 강력하게 보호해야만 한다.

5.3.2 정보의 제공 문제점 해결 방안에 대한 연구

쇼핑몰과 백화점등 기타 회원 가입 시 정보 주체의 불이익을 받을 수 있는 회원 가입 회칙이 우선적으로 바뀌어야만 한다. 또한 회원가입 직후라도 정보 주체가 적극적으로 사용에 대한 거부를 행사할 수 있도록 판매자 및 사용자의 동의 없이도 RFID의 기능적 사용이 이용되지 못하게 하거나 이용자체를 배제를 할 수 있는 권리가 부여되어야 한다. 즉 인식되지 않은 RFID Reader로부터 개인정보를 보호하기위해 RFID Reader 감지기나 전파 교란 장치(전파성이 약한 보호용)를 휴대하여 사용할 수 있는 권리를 부여하고, 개인 정보의 주체가 제공을 원하지 않는 개인정보가 포함되어 있다면 관련 RFID 태그를 스스로 제거하거나 기능 정지 또는 파괴할 수 있는 권리도 반드시 부여해야만 한다.

5.3.3 정보 관리 측면 해결 방안에 대한 연구

RFID가 활성화되면 적용되는 사업 분야에 관계없이 광범위한 정보수집이 가능하고 이런 정보는 손쉽게 취합되어 재분류할 수 있다는 점에서 RFID 관리자에게 책임범위를 확장하고 이에 대한 규제와 감독 등을 강화할 필요가 있다.

이 역시 위의 타 정보 시스템의 연결과 마찬가지로 이전 모 카드회사의 자료 제공, 인터넷 포털사이트의 고객정보 제공등 사회의 문제를 낳았던 부분이므로 정보 관리 측면에서 정보를 다루는 관계자들에 대한 교육 강화, RFID 사용에 대한 등록 및 홍보, 관리적인 측면에서 법제도적인 규제도 반드시 필요하다.

5.4 RFID 위치 정보 이용 측면 문제점

RFID는 초창기 개발부터 항공기의 아군식별을 위한

위치정보의 제공이 주요 목적 중 하나로 정보주체의 위치정보가 프라이버시 또는 개인정보 침해의 소지가 충분이 있었다.

특히 정보주체의 동의와 관계없이 개인정보의 위치정보를 알아낼 수 있으므로 RFID Reader가 있으면 상대방의 위치정보는 손쉽게 파악을 할 수 있으므로 이 또한 사회적 문제점이 매우 크다[15].

5.4.1 RFID 위치 정보 문제점 해결 방안에 대한 연구

위치 정보와 개인정보의 결합은 원칙적으로 강력히 규제되어야만 한다.

다만 긴급구조 등 정보주체의 생명과 관계된 긴급한 사항이라면 정보주체의 동의 없이도 위치정보가 제공된다는 것은 예외이다[15].

Ⅵ. RFID 보안 기술 비교 분석

지금까지 살펴본 RFID 개인정보 보안 문제점을 해결하기 위한 연구가 계속 진행되고는 있지만 아직 보안 요구 사항을 완벽하게 만족시킬 수 있는 방법은 없다. 그러므로 여러 가지 방법을 조합하여 사용하는 것이 현재로선 가장 좋은 방법이며, 본 논문에서는 이미 제안된 RFID 보안 기술에 대한 부분을 평가 분석<표 6>하여 제시하고자 한다.

6.1 RFID 태그의 무효화(Kill) 방법

RFID 태그 무효화 방법은 고객의 프라이버시 보호를 위한 가장 단순한 방법으로 상품이 고객에게 인도되기 전에 RFID 태그를 무효화(Kill)하는 것이다. 무효화된 태그는 다시는 Re-activated 되어 사용될 수 없다. AutoID 센터에 의해 제안된 동작의 표준 모드를 살펴보면 태그는 태그 부착 상품을 구매함으로써 무효화(Killed)되는 것을 의미한다[7].

6.2 Hash Lock 방법

태그에서 함수만을 구현하는 기법으로 총 6단계로 이루어졌으며, 하드웨어적 암호화나 보안 기능이 없으므로 위치추적, 재전송 공격, 스푸핑 공격 등에 매우 약하다.

그러므로 약한 Hash Lock을 개선하는 방안으로 태그에서 해쉬 함수, XOR, 연접연산을 사용하여 입력되는 문자열 정보를 잘게 쪼개 나누는 것이다.

<표 6> 보안 방식별 비교 분석

보안 방식	보안 요구도의 충족도			태그 연산	장점	단점
	태그보호	트래킹	전방위 안전성			
무효화(Kill)	일부 만족	만족	일부 만족	없음	구현이 용이	짧은 패스워드에 대한 공격의 위험성 존재
Hash Lock	만족	불만족	불만족	해쉬	구현이 용이	추적 기능, 태그 위조 가능
Randomized Hash Lock	만족	만족	불만족	해쉬, 난수발생	보안 요구사항 만족	난수 발생기의 구현 필요
External Re-Encryption	만족	만족	만족	없음	이론적으로 가장 안전	외부 유닛 필요 비현실적
Hash Chain	만족	만족	만족	해쉬	저가의 연산으로 보안 요구사항 만족	안전성 검증 미비, 저가의 해쉬 함수 구현
Sleep 명령과 Wake 명령	만족	만족	만족	없음	구현이 용이, 만족	태그 동작 및 키 관리에 따른 불편

그러면 데이터 전송 시 쪼개진 문자열 정보를 전송하게 될 경우 보안성이 강화될 수 있다[1].

6.3 Randomized Hash lock 방법

각 태그는 난수 생성기로부터 생성된 난수 값과 자신의 ID를 연접하여 해쉬 값을 계산한 후, Reader에 전송한다.

Reader는 개인의 태그 정보를 읽어 서버에 전송하는데, 서버에는 각 태그의 ID가 저장되어 있으므로 서버는 전송받은 데이터와 같은 값이 나올 때까지 모든 태그의 ID와 전송 받은 데이터를 비교하는데 실제로는 찾지 못해서 읽혀진 자료는 손실하게 된다[16].

6.4 External Re-Encryption Scheme 방법

인증기관에서만 추적이 가능하도록 인증기관의 공개키로 암호화하는 방식으로 주기적으로 태그 정보를 재암호화한다. 재 암호화된 보안은 보장이 되는 외부 기계를 통해서만 수행하게 되므로 매우 제한적인 연산 자원을 가지게 되어 가장 안전하다[16].

6.5 Hash Chain 방법

RFID 태그와 Reader기의 교신은 간단히 도청되기 때문에 그 통신에 암호화를 적용하여 허가되지 않는 불법 자료 제공업자로 부터 도청 또는 불법 수신되지 않기 위해서, RFID 태그 소유자나 특정 Reader기만 통신이 가능하도록 인증 및 암호를 이용하는 방법이다[7].

6.6 Sleep 명령과 Wake 명령어 방법

RFID 태그 무효화(Kill) 보안 기술의 단점을 보완하기 위해 개발된 기법으로 사용자의 태그 기능을 잠시 동안 정지한 후 안전한 장소에 이동하게 되면 다시 재가동되도록 하는 기법이다. 이 기능은 사용자가 각 태그의 동작 및 키 관리를 일일이 해야 하는 불편함이 따르긴 하지만 쉽고 안전한 RFID 보안기술로 널리 적용되고 있다[16].

Ⅶ. 결론

RFID 도입에 있어서 가장 중요한 문제는 무엇보다 개인정보 침해 문제이다. RFID 기술이 유비쿼터스 사회의 핵심 기술로 주목을 받는 것은 RFID 기술이 주는 편리한 혜택 때문이기도 하지만, 일반 사람들이 RFID 태그 인식 부족으로 자신들이 RFID 태그를 휴대함으로 언제, 어디서, 어떻게 자신의 정보가 읽혀지는지 조차 인지하기 못하기 때문에 편리함과 동시에 개인정보침해 위험성을 안고 있는 것이다.

이러한 편리함으로 인해 RFID는 물류, 유통, 재고관리, 운송관리, 출입통제관리, 자산관리 등에서 현재 널리 사용되어지고 있으며 점차 이용이 확대 예상되고 있다. 그러나 각 산업현장에서 RFID 사용에 대한 분포가 증가함에 따라 개인정보침해에 대한 문제의 소지도 증가될 것으로 예상되어진다.

앞으로 사회적으로 RFID에 대한 개인정보 침해 문제에 대한 기술적, 제도적 문제점 등에 대한 대책이 마련되지 않는다면 사용 분포에 따른 긍정적 파급효과는 어려워질 수도 있다.

본 논문에서 평가 분석한 제시 모델의 핵심 보안 기술인 External Re-Encryption Scheme 방식과 Sleep and Wake 보안기술 등을 잘 활용한다면 고객들이 인지하지 못한 상황에서도 무선 전파를 이용한 RFID 리더들이 개인정보 불법 자료 수집에 대한 취약성을 어느 정도 해결할 수 있을 것이다.

향후 RFID 개인 정보 보안 기술 보급으로 인한 기대효과는 정부, 공공기관의 RFID 인프라 구축으로 인한 고용 창출 효과, 총생산 유발효과, 부가가치 유발효과 등 사회적, 경제적, 기술적 영향을 미치는 성장이 예상된다.

참고문헌

[1] 김대중, 전문석, “일회성 난수를 이용한 안전한 RFID 상호인증 프로토콜 설계,” 한국정보과학회, 정보과학회논문지 제35권, 제3호, 2008, pp. 243-244.

[2] 노영, 변정우, “RFID를 활용한 유비쿼터스 컨벤션에 관한 연구,” 디지털산업정보학회, 디지털산업정보학회논문지 제5권, 제3호, 2009, pp. 176.

[3] 김동성, 박종서, “RFID/USN 보안 연구대상 및 향후추세,” 한국정보과학회, 정보보호학회지 제15권, 제1호, 2005. 2.

[4] 김광조, “RFID/USN 정보보호기술,” TTA저널, 제95호.

[5] 이근호, 한호헌, 강병권, 조영빈, “유비쿼터스 핵심 RFID,” 영진닷컴, 2005.

[6] 조희석, “RFID와 개인 정보 보호,” IT Solutions, 2005.

[7] ETRI, “유비쿼터스 환경에서의 개인정보 보호 기술,” 2005.

[8] 한국정보보호진흥원, “개인정보 취급 방침 예시,” 2007.

[9] 유비유넷, “RFID와 프라이버시,” 2006.

[10] 전자정보센터, “IT리포트 : RFID 시스템의 보안 및 프라이버시 보호를 위한 기술,” 2004.

[11] KETI 전자부품연구원, “RFID(Radio Frequency IDentification),” 2005.

[12] 정보통신부, “RFID 프라이버시 보호 가이드라인,” 2005.

[13] 구병문, “NCA CIO REPORT : RFID 도입과 프라이버시 보호 관련 법제 현안 분석,” 한국전산원, 2004.

[14] http://www.index.go.kr/egams/index.jsp

[15] http://privacy.kisa.or.kr/privacy/jsp/pr_1.jsp

[16] http://www.csokorea.org/sub04_view. asp?idx=2394&page=8&search=&searchstring=&kind=03

■ 저자소개 ■

최 희 식
Choi, Hee Sik

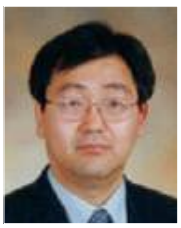
2006년 3월~현재 승실대학교 일반대학원 컴퓨터학과 박사과정
2006년 2월 승실대학교 컴퓨터공학과(공학석사)
2008년 경원대학교 출강
2008년 경민대학교 출강
2007년 승실대학교 전산원 출강
2007년 삼육대학교 출강

관심분야 : DRM, 유비쿼터스, RFID
E-mail : dali3054@ssu.ac.kr

박 재 표
Park, Jae Pyo

2010년 3월~현재 승실대학교 교수
2008년 9월~2009년 8월 승실대학교 정보미디어기술연구소 전임연구원
2004년 8월 승실대학교컴퓨터과학과(공학박사)
1998년 8월 승실대학교 컴퓨터학과(공학석사)
1996년 2월 승실대학교 컴퓨터학부(공학사)

관심분야 : 컴퓨터보안, 유비쿼터스, 컴퓨터통신
E-mail : pjerry@ssu.ac.kr



전 문 석
Jun, Mun Seog

1991년 3월~현재 승실대학교 컴퓨터학과 교수
1989년 Morgan State University(조교수)
1989년 University of Maryland Computer Science(공학박사)
1988년 University of Maryland omputer Science(공학석사)

관심분야 : 정보보호, 네트워크보안, 암호학
E-mail : mjun@ssu.ac.kr

논문접수일 : 2010년 4월 30일
수 정 일 : 2010년 5월 20일
게재확정일 : 2010년 6월 8일