

RFID 기반의 교육 케어 시스템 구현

김나훈*, 홍진근*, 한군희*
*백석대학교 정보통신학부
e-mail: knh031@nate.com

Implementation of Education Care based on RFID

Na-Hoon Kim*, Jin-Keun Hong*, Kun-Hee Han*
*Division of Information Communication, Baekseok University

요 약

우리나라의 사교육기관인 학원의 수가 증가하고 그에 따른 학생들의 수도 증가함에 따라 관리자측면에서 학생관리 시스템의 변화가 제기되고 있고 특히 학생들의 등하교에 따른 출결여부와 학부모에게 공지사항을 전달하는데 많은 시간적, 경제적 비용이 소모되고 있는 실정이다. 이러한 문제를 해결하기 위하여 본 논문에서는 최적화된 RFID기술에 관해 연구하였다. RFID리더기를 이용하여 학생들의 출결여부를 실시간으로 입력함으로써 학생 관리를 하는데 있어서 시간과 노력을 줄일 수 있는 RFID기술 기반의 학원관리 시스템을 구현하였다. 실시간으로 SMS메시지 전송서비스를 제공하였으며, Tag를 인식 할 때 해쉬기반의 인증 메커니즘을 추가하여 구성하였다.

1. 서론

교육 분야와 관련된 케어 서비스는 U-School 실현을 위한 학원 관리시스템 및 제반 교육환경을 구축하는 서비스이다. 학원 케어의 첨단 학생관리 프로그램과 장비를 통해 학원의 공지사항이나, 알림사항을 학부모의 휴대폰으로 전송할 수 있고, 학원케어의 전자(RFID)학생증을 이용하여 학생의 등, 하교 상황도 역시 휴대폰을 통해 문자로 확인할 수 있다. 그 외, 수납관리, 통학차량 이용 등 학원에서 필요로 하는 시스템에 접목하여 활용할 수 있다. 학원 케어 서비스는 미래교육환경의 U-School 실현은 물론, 어린이 안전에 대한 보험서비스까지 제공함으로써, 사교육의 내실화와 학생들의 안전까지 지키는 교육기관에 꼭 필요한 서비스이다[1].

RFID 기술은 사물에 부착된 태그로부터 전파를 이용하여 사물의 정보 및 주변 환경을 인식하여 각 사물의 정보를 수집, 저장, 가공, 추적함으로써 사물에 대한 측위, 원격 처리, 관리 및 사물 간 정보 교환

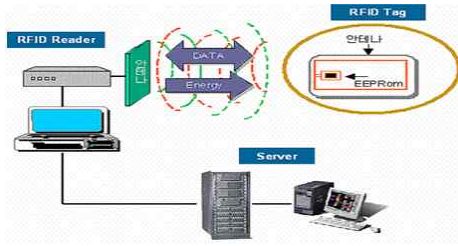
등 다양한 서비스를 제공할 수 있다. 이러한 기술은 기존의 바코드를 대체하여 물품 관리를 네트워크화 및 지능화함으로써 유통 및 물품 관리뿐만 아니라 보안, 안전, 환경 관리 등에 혁신을 선도할 것으로 전망되며[2], 특히 교육 분야에서 RFID Tag로 제작된 전자학생증을 활용함으로써 교육기관 시스템의 향상과 함께 이전에 존재하지 않았던 거대한 새로운 시장을 형성할 것으로 기대된다.

본 논문에서는 RFID 기반의 학원 케어 시스템 구현 대하여 설명하고자 한다. 2장에서는 RFID 시스템의 구성과 동작과정 그리고 Tag 인증기술에 대하여 알아보고 3장에서는 본 논문에서 제안하는 RFID 기반의 학원 케어 시스템 구현에 대하여 설명하고 4장에서는 결론 및 향후 연구방향에 대해서 설명한다.

2. 관련연구

2.1 RFID 시스템의 구성

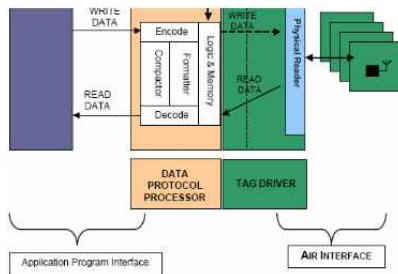
RFID 시스템은 세가지 주요 요소로 구성된다. 추적에 필요하거나 식별이 필요한 물품에 부착되는 태그, 태그에 전원을 공급 및 식별, 데이터 읽기 및 쓰기, 데이터 수집 응용 서비스를 관리하는 리더와 리더로부터 데이터 수집, 데이터베이스로의 정보입력, 수혜기관에 유용한 형태의 데이터 접근 기능을 제공하는 서버이다[3].



<그림 1> RFID 시스템 구성도

2.2 RFID 동작과정

RFID시스템의 동작과정은 다음 1단계에서부터 6 단계로 구성하였다



<그림 2> RFID 동작과정

1단계, RFID 리더는 RF 필드에 구성된 안테나에서 무선 신호를 생성하고 전파한다. 2단계, RF field를 통과하는 태그는 적합한 무선신호를 수신한다. 3단계, 무선신호는 태그의 자체 안테나에서 수신된다. 4단계, 태그의 칩은 에너지를 공급받고 사전 프로그램 된 데이터(고유 식별자)를 전송한다. 5단계, 무선신호의 일부가 변조되고 리더로 반향[Reflected]된다. 6단계, 리더는 반향 된 신호를 변환(decode)하고 데이터 수집 장치와 host 시스템으로 전달한다.

2.3 RFID 인증 프로토콜

RFID 시스템에서는 리더를 소유한 공격자는 물리적인 접촉 없이 태그의 정보를 읽는 것이 가능하

로, 사용자가 알지 못하는 사이에 태그에 저장된 정보가 노출되거나 태그의 식별 정보를 이용한 사용자의 위치 추적 등이 가능하게 된다. 본 절에서는 지금까지 제안된 인증 프로토콜을 살펴보고자 한다.

2.2.1 해쉬 락(Hash lock) 프로토콜[3]

해쉬 락 프로토콜은 “locked” 상태에서는 태그가 자신의 실제 ID 값이 아닌 metaID 값을 전송하고, “unlocked” 상태에서만 실제 ID를 전송함으로써 사용자의 프라이버시를 보호하는 방식이다.

2.2.2 확장된 해쉬 락 프로토콜[3]

랜덤화 된(randomized) 해쉬 락 방식으로 태그는 해쉬 함수를 이용하며 매 세션마다 전송되는 값을 변형하며 공격자나 리더를 포함한 허가받지 않은 개체에 의한 트래킹을 방지할 수 있다.

2.2.3 외부 재 암호화(Re-encryption)을 이용하는 방식[4]

태그의 메모리는 optical contact area와 RF contact area로 나누어지며, 리더에 의해 태그가 인식된 후에 재 암호화를 이용하여 태그에 저장된 정보를 재 기록하는 방법이다.

2.2.4 해쉬 체인(Hash-chain)을 이용하는 방식[4]

해쉬 체인을 이용하는 방식은 두 개의 해쉬 함수를 이용하여 리더의 query에 대해 태그가 매 세션마다 서로 다른 응답을 전송하고, 이를 이용하여 태그를 인증하는 방식이다.

2.2.5 해쉬 기반 ID 변형 프로토콜[4]

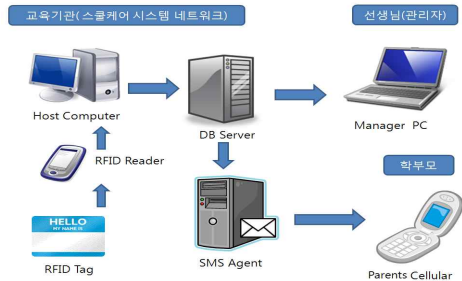
해쉬 기반 ID 변형 프로토콜은 매 세션에서 난수를 생성하고 이를 이용하여 인증 정보를 매번 갱신 하므로 공격자로부터 프라이버시를 보장 받을 수 있다.

3. RFID 기반의 학원 케어 시스템

3.1 학원 케어 시스템 구성

제안된 교육 케어 시스템은 학원 환경에 적합하도록 구성하였다. 전자학생증인 RFID 태그를 각 강의 실입구에 있는 RFID 리더로부터 정보를 읽고 호스트 컴퓨터가 데이터베이스 서버로부터 태그정보와 일치하는 학생DB 검색하여 출결정보를 입력한 후 해

당 정보는 관리자 또는 담임선생님이 클라이언트 프로그램으로 쉽게 확인 할 수 있도록 구성하였다. 또한 DB정보를 SMS 전송서비스를 이용하여 출결유무를 비롯한 공지사항 및 안내 메시지를 즉시 학부모 핸드폰으로 전송함으로써 학부모가 학생의 출결 여부 및 각종 정보를 확인 할 수 있다.



<그림 3> 학원 케어 시스템 구성도

3.2 RFID 인증 메커니즘

인증방안을 <그림4>처럼 제안한다. 태그 리더는 태그에 query 전송하고 태그는 저장된 태그식별번호인 UID, RFID 리더기 GPS의 위치 좌표값, GPS 데이터 시간값을 TS로 하여 해쉬 기술인 SHA-256[5]을 사용하여 해쉬값과 랜덤값을 리더에 보낸다. Reader는 DB에 UID를 전송하고 DB는 해당하는 Key, ID를 리더에 전송하고 리더는 태그에 Key값을 전송하면 Tag는 key값을 확인후 ID정보를 전송한다.



<그림 4> RFID 인증 메커니즘 구성도

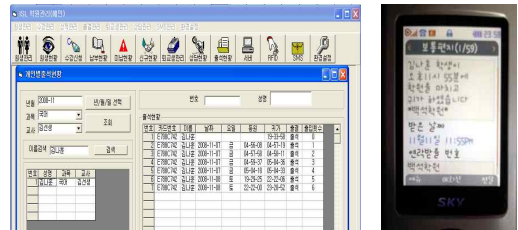
3.3 시스템 구현 결과

구현된 제안 시스템은 <그림5>와 같이 RFID Tag 정보를 Read/Write 할 수 있도록 설계하였다.



<그림 5 > RFID Information

관리자는 구현된 프로그램을 통해 <그림 6> (a) 학생들의 출결 여부를 실시간으로 확인 할 수 있다. 구현된 프로그램은 SMS Agent를 통해 해당 학부모 핸드폰<그림6> (b) 으로 출결여부를 실시간으로 전송한다.



a.개인별출석현황 화면 b.전송 SMS 화면

<그림 6 > GUI 인터페이스 화면

4. 결론 및 향후 연구방향

본 논문에서는 RFID를 활용하여 학원관리 프로그램을 구현하였다. 구현을 위해 RFID Tag Read/Write, RFID Reader 와 호스트 PC간 시리얼 통신 인터페이스 설계, 호스트PC와 DB Server 간 Oracle Query작성, SMS Agent를 통한 SMS 전송서비스를 구현하였다. 구현된 시스템을 활용하여 학생들의 출입정보 및 데이터 관리 그리고 학부모에게 공지사항 전달을 손 쉽게 할 수 있었다. 프로그램을 웹으로 구현, 태그를 통한 위치 탐지, 개인 프라이버시 보호를 위한 RFID 보안 솔루션 제공을 위한 연구가 필요하다.

참고문헌

- [1] Broad&SchoolCare, <http://uschool.bizfos.co.kr/kidscare31.asp>
- [2] 최길영, 성낙선, 모희숙, 박찬원, 권성호, "RFID 기술 및 표준화 동향", 전자통신동향분석 제22권 제3호 2007년 6월
- [3] 박종대, 김현석, 최진영 "RFID 인증을 위한 해쉬 함수 기반의 네트워크 보안 프로토콜", 2006한국컴퓨터종합학술대회논문집
- [4] 오수현, 광진, "전자 태그의 보안 레벨을 기반으로 하는 RFID인증 프로토콜", 한국통신학회논문지 '05-6Vol.30 NO.6C
- [5] Hui Li, Yibin Hou, Zhangqin Huang, He Fugui, Chen Rui, "An Authentication RFID Reader with FPGA", (ICCESS2008)