

스마트 홈 서비스를 위한 스마트 원격 도어락 제어 모듈

구유탉, 신은재, 장휘수, 정기면, 한현관, 고정호
영진전문대학 컴퓨터정보계열

e-mail : flyiceball@gmail.com, , hanhyoun@daum.net, jhkont@yjc.ac.kr

Smart Remote Doorlock Control Module for Smart Home Services

Yuntack Koo, Eunjae Shin, Gimyung Jung, HwiSoo Jang, Hyunkwan Han, Jeongho Ko
Dept. of, Youngjin College

요 약

최근 ‘도어락 몰카’와 같은 생활 보안범죄가 잇따라 증가함에 따라 해결법으로 판넬에 비밀번호를 직접적으로 입력하지 않는 방식을 아이디어로 채택하여 도어락의 비밀번호 유출위험과 판넬에 직접 입력하는 번거로움을 없이 도어락을 열 수 있는 방식을 도입하고자 한다. 원격으로 제어 하는 방식은 해킹의 위험이 있으므로 보안모듈을 도입하여 해킹의 위험을 감소 시키는 방법을 연구하고자 한다. 이를 위해 암호화 모듈, 아두이노의 블루투스 및 Wi-Fi통신, 모터를 이용한 도어락 제어를 할 수 있도록 하여 궁극적으로 스마트 홈 서비스를 구축 하고자 한다.

1. 서 론

현관문 위에 화재경보기처럼 생긴 몰래 카메라를 설치, 비밀번호를 알아내 아파트를 털어온 도둑이 붙잡혔다. 서울 송파경찰서는 아파트 현관 위 천장에 몰카를 설치해 집 주인이 현관 비밀번호를 누르는 모습을 녹화한 뒤 빈집에 들어가 금품을 훔친 혐의(상습절도 등)로 김모(49)씨를 구속하고 공범 고모(37)씨의 뒤를 쫓고 있다고 23일 밝혔다.[1] 이러한 ‘도어락 몰카’와 같은 범죄의 증가에 따른 불안요소들이 증가하고 있다. 이에 따른 대안과 편의성 증대의 목적으로 원격 도어락 잠금 해제 장치가 속속히 개발되고 있다.[2,3]

하지만 기존의 스마트 도어락들은 비싼 가격과 기존의 도어락을 떼어내고 새롭게 부착하는 형식의 방법으로 추가적인 시공이 필요로 하였다.[4] 본 논문에서는 그러한 문제점을 해결할 방법으로 모듈 형식의 장치를 이용하여 일반 도어락을 스마트 도어락으로 바꾸는 방식을 개발하였다. 그리고 원격으로 제어 하는 방식에는 해킹의 위험이 존재하기에 KISA에서 제공하는 LEA암호화 라이브러리를 이용하여 독자적으로 개발한 보안 모듈을 적용 하였다.

블록암호 LEA(Lightweight Encryption Algorithm)는 128비트 데이터 블록을 암호화하는 알고리즘으로 128, 192, 256비트 비밀키를 사용할 수 있으며 요구되는 안전성 기준에 따라 용도가 구분될 수 있다. LEA(Lightweight Encryption Algorithm)의 라운드 함수는 32비트 단위의 ARX(Addition, Rotation, XOR) 연산만으로 구성되어 있어, 이들 연산을 지원하는 범용 32비트 소프트웨어 플랫폼에서 고속으로 동작한다. 또한 라운드 함

수내부의 ARX(Addition, Rotation, XOR) 연산 배치는 충분한 안전성을 보장하는 것과 동시에 S-box의 사용을 배제하여 경량 구현이 가능하도록 한다.[4]

제안한 장치는 도어락 뿐만 아니라 감지 센서를 도입하여 도어락 만이 아닌 자동문과 같은 장치로의 확장을 기대 할 수 있다. Wi-Fi 및 블루투스를 이용한 원격 제어, 장치를 이용하여 연 기록들을 기록하는 로그기능, 소형화 및 장시간 이용을 위해 아두이노를 사용하고 구동부분은 큰 힘이 필요 없고 제어가 간단한 서보모터를 사용하였다.

본 논문의 구성은 다음과 같다. 2장에서 제안하는 스마트 도어락을 소개하며, 3장에서 개발 시스템의 실험 결과를 설명한다. 마지막으로 4장에서는 본 논문의 결론 및 향후 연구 방향에 대하여 서술한다.

2. 스마트 도어락의 구성 설명

2.1 모듈 장치의 구성

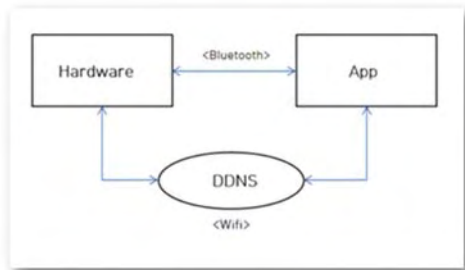
기존의 도어락 위에 장치를 부착하여 서보모터를 통하여 도어락의 개폐 장치를 누르는 방식으로 도어락의 잠금 상태를 제어



[그림 1] 구성도

2.2 네트워크 구성

아두이노를 제어하는 방법은 블루투스와 Wi-Fi를 통한 두가지 방식 모두를 제공한다. Wi-Fi의 경우는 외부 서버가 아닌 DDNS를 지원하는 공유기를 이용하여 DDNS를 사용한 접속방법으로 한다.



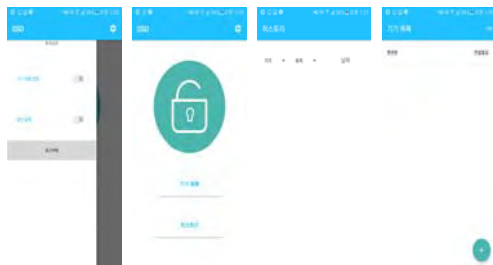
[그림 2] 네트워크 구성도

3. 개발 시스템 결과 및 보고

이 장에서는 2장에서 제안한 시스템의 개발 현황과 문제점 및 해결에 대하여 설명한다.

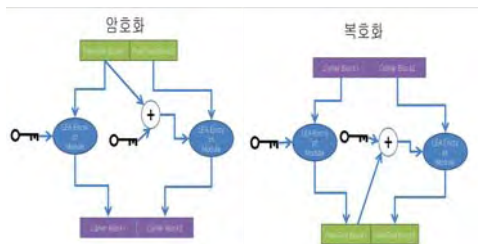
3.1 시스템 개발 과정

① 아래의 그림 3은 본 시스템에서 개발 중인 앱의 구현된 UI에 관한 그림이다. 왼쪽부터 환경설정, 메인화면, 히스토리, 기기등록 및 관리에 관한 화면이다.



[그림 3] UI

② 아래의 그림 4는 시스템의 암호화와 복호화 모듈의 그림이다. 256비트 고정크기의 패킷을 128비트씩 블록 암호화 하는 방식으로 평문과 키를 Xor 연산을 하여 다음 세션키를 만드는 방식이다.



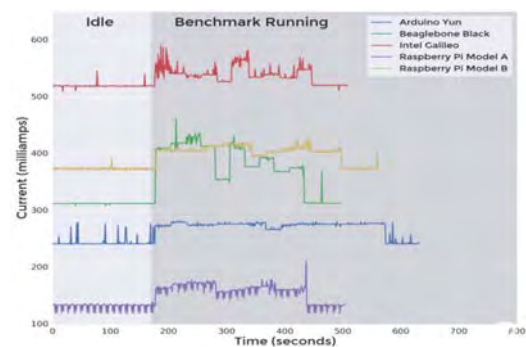
[그림 4] 암호화와 복호화 모듈

3.3 문제점 및 방안

아래의 그림 5는 아두이노들의 전력 비교 그림 6은 아두이노 운의 전력소모량이 적혀 있는 그림이다. 그림 5의 아두이노 Uno와 비교하여 아두이노 운은 2배 가까운 전압을 사용하여 전력 소모량이 더 높은 것을 확인할 수 있다. 제한한 시스템의 전력 소모량이 큰 문제점으로 다가 올 것이라고 예상할 수 있다. 이 문제를 해결하기 위하여 Sleep 모드 등의 코드 상에서의 전력 소모를 줄이는 방향을 모색하고 있다.

	Uno	Nano	Mega	101
Revision	R3	R3	R3	R1
CPU	ATmega328	ATmega328	ATmega2560	Intel Curie
Voltage	5.10V	5.10V	5.10V	5.10V
Program #1 Current	144mA	35mA	79mA	66mA
Program #1 Power	734mW	179mW	403mW	336mW
Program #2 Current	144mA	35mA	81mA	68mA
Program #2 Power	734mW	179mW	413mW	347mW

[그림 5]전력 소모량



[그림 6] 전력 소모

4. 결론 및 향후 연구 방향

4.1 비교 분석

일반 도어락을 스마트 도어락으로 바꾸는 방식을 개발하였다

	스마트 도어락	일반 도어락	제안 시스템
Wi-Fi 잠금 해제	X	X	O
블루투스 잠금 해제	O	X	O
로그	X	X	O

4.2 결론

현재 시중에 나온 스마트 도어락과 비교하여 Wi-Fi잠금 해제 및 블루투스 잠금 해제 와 로그 기능 까지 모두 지원하는 장치는 논문의 제안한 시스템뿐이다. 이러한 부분을 보았을 때 제안 시스템의 발전 가능성은 매우 높은 편이다.

“본 논문은 2017년 한이음 ICT멘토링 프로젝트의 결과물입니다.”

5.참고 문헌

- [1] "우리집 현관위에 몰카가?"...비밀번호 알아내 아파트 털어(연합뉴스)
<http://www.yonhapnews.co.kr/bulletin/2015/08/22/0200000000AKR20150822062500004.HTML>
- [2]<http://robilitive.com/1905>
- [3]<http://blog.naver.com/PostView.nhn?blogId=sbkim24&logNo=220957629429>
- [4]<https://seed.kisa.or.kr/html/egovframework/iwt/ds/ko/ref/LEA%20A%20128-Bit%20Block%20Cipher%20Datasheets-Korean.pdf>
- [그림5]<https://tlextrait.svbtle.com/arduino-power-consumption-compared>
- [그림6]<https://learn.adafruit.com/embedded-linux-board-comparison/power-usage>