Proceedings of KFIS Spring Conference 2005 Volume 15, Number 1

암호화 알고리즘을 이용한 출입문 제어 시스템에 관한 구현

A Study on the gate control system using password algorithm

이봉우, 최우경, 김성주, 김용민*, 전홍태
중앙대학교 전자전기공학부
*충청대학 컴퓨터학부

Bong-Woo Lee, Woo-Kyung Choi ,Seong-Joo Kim, Yong-Min Kim* ,Hong-Tae Jeon
School of Electrical and Electronic Engineering, Chung-Ang University
*Dept. of Computer Science, Chung-Cheong University
E-mail :bong400@hotmail.com

요 약

과학이 주는 가장 큰 이점인 인간의 편리함을 추구하는데 있어서 자동화라는 개념을 빼놓을 수는 없을 것이다. 특히 인간생활의 기본이 되는 가정에서의 편리성은 항상 최우선 되어져 왔다. 본 논문은 미래 사회 핵심 기술인 자동화의 가장 근본이 되는 Home Automation에 암호화 알고리즘을 통한 출입문 제어 시스템의 구현과 유비쿼터스의 개념을 도입하는 것에 그 목적이 있다. 현재까지 출입문 제어 시스템에 관한 수많은 논의와 연구가 이루어 졌지만 기존의 키 인증 방식은 한계가 존재하였다. 이에 인증서 개념 도입을 통한 암호화 알고리즘을 선보이고 기존의 키 인증시스템의 문제점을 해결하고 보안상의 문제도 해결 하는 방법을 제안한다.

1. 서론

다가오는 세계는 유비쿼터스 시대이다. 유비쿼터스란 사용자가 시간과 장소에 구애 없이 언제 어디서든 간편하고 자유롭게 네트워크에 접속 할 수 있다는 것을 의미한다 [1][2]. 책, 침대, 의자, 보일러, 차량, 냉장고, 전등, 모든 사물이 디자인을 가지듯이 유비쿼터스는 모든 사물에 칩을 가지게 한다. 그 칩은 RFID라고 하며 1㎤이하의 크기로 만들어지는 저 전력 칩이다. 칩이 깃들게 되는 사물은 모두 컴퓨터가 되며 우리는 컴퓨터 속에서 살게 된다. 유비쿼터스의 의미를 살펴보면 유비쿼터스는 정보 통신 관점에서 모든 사회분야에 대한 새로운 패러다임을 창조하는 것이다. 모든 것은 유비쿼터스적인 관점에서 새롭게 해석되어야 한다. 그 분야는 특정 분야가 아니며 기존의 사회에 구성되어 있는 모든 분야를 포함한다. 컴퓨터가 있을 때와 모든 분야에서 컴퓨터가 적용될 때를 생각하면 비슷할 것이다. 또한 현재 전 세계적으로 자동화에 대한 광범위한 연구가 이루어지고 있으며 가정에서의 자동화는 모든 자동화의 근원이 되므로 우선적인 논의가 되고 있다. 자동화

와 유비쿼터스는 현재 주축이 되는 연구 부분이며 이 둘을 접목하여 지금까지 물리적으로만 이루어졌던 출입문 제어 시스템을 자동화로 구축한다는 발상에 개인 단말기(Personal Mobile Terminal;PMT)의 무선통신(Wireless Communication)기능을 이용하여 유비쿼터스 방식의 개념을 도입하고 제어와 출입함에 있어서 인증서 개념으로 로그파일을 생성하여 출입에 관한 기록을 작성 방식을 이용한 사용자의 보안에 대한 문제까지 해결하고자 한다.

현재 입 출입 시스템의 경우에서 발생하는 불리함은 반드시 물리적 Access가 필요하다는 것이다. 앞의 유비쿼터스의 내용을 보면 자동화 Access가 중요 기술력의 하나이다[3][4]. 또한 보안성 문제에서도 불리함이 존재한다. 앞으로 구현의 우선은 바로 이 물리적 Access를 없애고 보안상의 문제점을 해결한다는 것이다. 이런 문제점을 해결한다면 보다 나은 키 인증 시스템을 구축할 수 있다는 것이다. 본 논문의 구성은 다음과 같다. 암호화 알고리즘에다 인증서 개념을 소개하고 자동화된 유비쿼터스 기기를 이용하여 시뮬레이션 한 결과를 구현해 보이고자 한다.

2. 암호화 알고리즘과 인증서

2.1 암호화 DES Algorithm

알고리즘 구현에 있어서 가장 우선 이루어져야 하는 문제가 바로 암호화이다[5][6]. 기본적으로 암호화 모듈을 적용하여 구현해야 하기 때문에 DES 알고리즘을 사용한 암호화 및 복호화가 가능해져야 한다[7]. 암호화 및 복호화 과정을 확인하기 위해 크게 4창으로 분류하였다. 평문을 입력하고 키를 입력하면 이를 암호화하여 나타내주는 창이 필요하고 암호화 된 문장을 다시 복호화해 주는 과정을 보여주는 창, 그리고 복호화 된 문장을 보여주는 창이 필요하다. 암호화 과정에서 키 스케줄을 확인하는 창을 따로 구현하여 키 스케줄이 16번의 반복동안 정확히 구현되는지도 확인하였다. 이 과정에서 암호화 과정을 다시 따로 분리하여 임베디드 C++을 이용하여 PDA에 적용하기로 했다. PDA에서 서버로 전송 시 암호화된 패스워드를 보내줘야 하기 때문에 PDA 상에서도 암호화 모듈이 필요하다. 위에 DES 알고리즘을 확인해보면 64비트 단위로 끊어서 8개의 킷값과 16번의 반복을 통해서 최종 구현된다. 그러기 위해서 우선 데이터를 2진수로 변환해야 할 필요가 있다. 따라서 입력된 데이터를 64비트 단위로 끊어서 2진수로 변환하는 과정이 필요하다. 이 과정이 해결되면 준비된 키 알고리즘과 함께 16회 변환과정을 통해서 최종적으로 암호화된 문장이 완성되게 된다. 복호화 하는 과정은 입력된 이 데이터를 다시 2진수로 변환 동일한 키 스케줄을 통해 역변환 과정을 거쳐 최종적으로 입력한 데이터와 동일한 값을 만들어내는 것이다. 암호화된 패스워드를 PDA에서 서버로 전송하게 되면 보안적인 면에서의 문제점을 해결할 수 있다.

2.2 인증 로그파일 생성

최종적으로 구현된 환경에 로그파일을 생성하여 사용자가 접속한 시간을 갱신하기로 하였다. 이는 보안적인 측면에서 사용자의 출입 현황을 기록함으로서 기존에 보안에 취약한 문제를 해결하기 위함이다.

무선 랜 방식을 적용하여 불필요한 엑세스를 없애고 보안상의 문제는 암호화 알고리즘을 적용하여 효율적으로 개선할 수 있다. 또한 인증서 개념 도입으로 사용자의 데이터베이스를 보다 효율적으로 활용 정확한 사용자를 인식하는데 성공 할 수 있다. 이 인증서 개념을 좀 더 개선해서 차후에 호환성 문제를 해결한다면 금융업무나 기타 기능에 대한 가능성도 충분하다.

3. 시스템 구성

아래 그림는 본 논문에서 제안한 시스템

전체 구상도 이다.

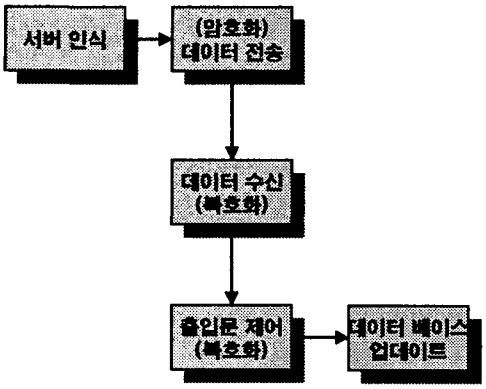

그림 2. 전체 시스템 구상도

아래 알고리즘은 본 시스템에 사용된 암호화 알고리즘 중 DES 알고리즘에 대한 그림이다.

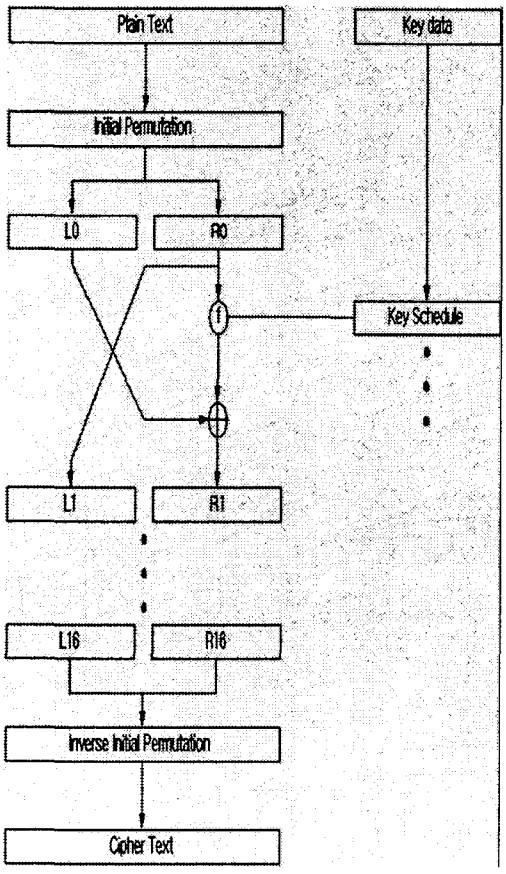

그림 3. DES 알고리즘

PDA를 이용하여 암호화를 이용한 출입문 제어 알고리즘을 구현 해 보았다.

킷값과 저장된 패스워드를 가지고 있다. 클라이언트에서 전송된 패스워드를 가지고 있는 킷값을 이용해 복호화 하고 가지고 있는 패스워드와 비교하여 사용자를 인증한다.

현재 시각을 얻어 서버 유저파일에 저장해 주고 PDA에도 전송하여 유저 파일에 저장한다. 따라서 최종접속 시간을 확인할 수 있다. 보안성의 문제를 해결하는 한 방법이다.

PDA의 경우 소켓통신에 연결과 해제과정을 보여주기 위해 버튼을 생성하였고 PASSWORD 입력을 위해 에디트 창을 설정하였다. 에디트 박스에 소켓이 연결되었는지를 표시하였고 문이 열릴 경우 혹은 PASSWORD가 틀릴 경우 해당 명령어를 표시 하도록 하였다.

그림 3은 본 시스템의 전반적인 구성도이다. 그림 4와 그림 5는 암호화 알고리즘을 PDA 상에 직접 구현한 모습이고, 그림 6은 인증 로그 파일을 보여주는 그림이다.

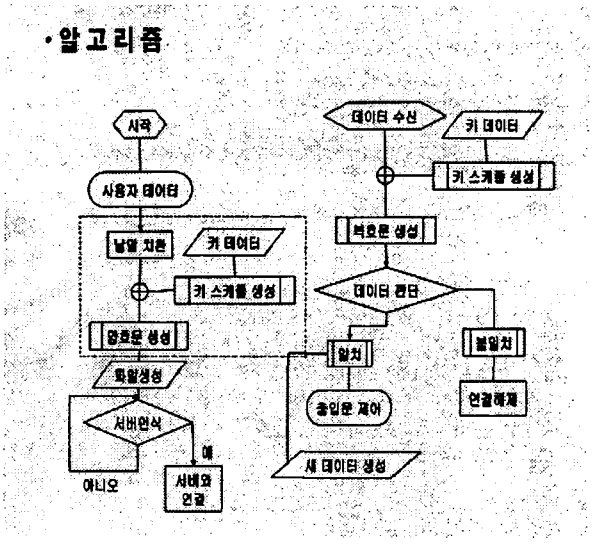

그림 4. 시스템 알고리즘

4. 시뮬레이션

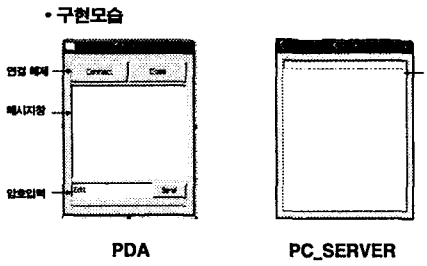

그림 5 PDA 와 서버 모습

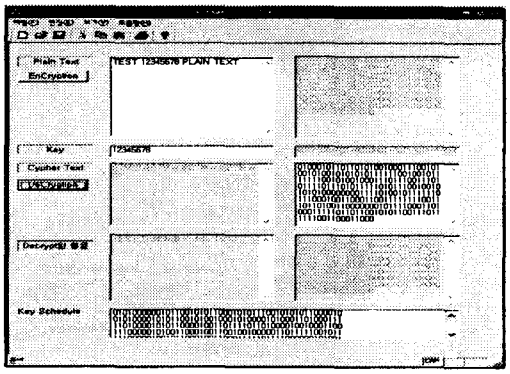

그림 6. 암호화 과정 구현 모습

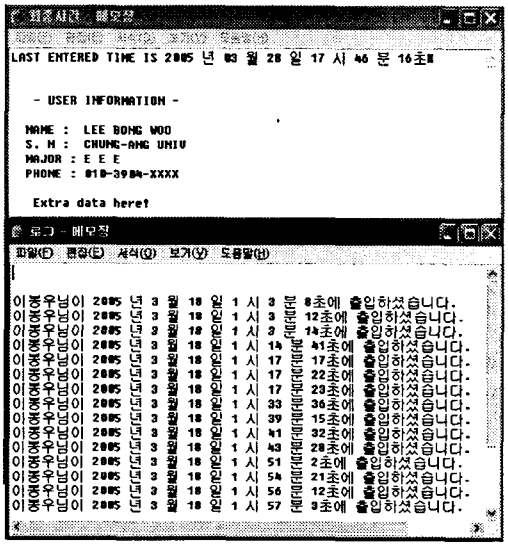

그림 7. 인증 로그파일 생성과 최종시간

5. 결론 및 향후 과제

최종적으로 구현한 모델의 기본 목적은 기존의 키 인증 시스템의 문제점을 해결하자는 것이었다. 가지고 있는 문제점의 물리적 엑세스의 필요 그리고 보안상의 문제 마지막으로 인증서 개념의 도입이었다. 무선랜 방식을 적용하여 불필요한 엑세스를 없앴고 보안상의 문제는 암호화 알고리즘을 적용하여 효율적으로 개선하였다. 또한 인증서 개념 도입으로 사용자의 데이터베이스를 보다 효율적으로 활용 정확한 사용자를 인식하는데 성공했다. 이 인증서 개념을 좀 더 개선해서 차후에 호환성 문제를 해결한다면 금융업무나 기타 기능에 대한 가능성도 충분히 가지고 있다. 더 이상의 물리적 키 개념이 아닌 보안성까지 고려한 키 인증 시스템의 구축으로 앞으로의 사회에 사용될 시스템을 도입해 보았다고 생각하고 유비쿼터스 시스템에서의 적용을 기대한다.

감사의 글 : 본 논문은 산업자원부의 차세대 신기술 개발사업에 의해 지원받았습니다.

6. 참고문헌

[1] 권오병, 정기욱, 유비쿼터스 시스템의 이해, 신론사, 2004.

「2」 김재윤, 유비쿼터스 컴퓨팅 :삼성경제연구원,2003.

[3] Bisgrove, J. Dayao. R. Houser, B. Jones, T. Mayes, J.C. McGinnis,M. Schmidt, M. Skyles, G. Tan,B.K. "Integrated test facility (ITF)-automation testing to support Intel's manufacturing output", *IEEE International Symposium,* PP,D17-D21,OCT.,1977

[4] Parasuraman, R.; Sheridan, T.B.; Wickens, C.D.;"A model for types and levels of human interaction with automation", *IEEE Transactions,*VOL.30,ISSUE3,PP.286-297,2000.

「5」 한국전자통신 연구원, 한국암호학의 기초,경문사,1999.

「6」 김철, 암호학의 이해,영풍문고,1996.

「7」http://realtime.ssu.ac.kr/wiki/kis2u_2fopensource_2fdes