韓國컴퓨터情報學會 論文誌
第16卷 第2號, 2011. 2.

2011-16-2-4-4

스마트폰을 이용한 원격 물리적 보안 시스템의 구현

이 문 구*

Implementation of Remote Physical Security Systems Using Smart Phone

Moon-Goo Lee*

요 약

기존의 유선상의 물리적 보안 시스템은 시간적, 공간적 제약을 갖는다. 이러한 문제점을 해결하기 위해서 본 연구는 스마트폰을 이용한 원격 물리적 보안 시스템을 구현 하였으며, 연구는 모바일 클라우드 컴퓨팅 기술을 기반으로 구현되었다. 모바일 클라우드 컴퓨팅 기술에서 요구되는 사용자 인증, 통신의 비밀성, 정보의 무결성, 시스템의 가용성, 접근제어 및 권한관리 그리고 안전한 핸드오프 등의 보안 기술을 구현하였다. 구현된 시스템은 계측, 감시, 제어를 통한 에너지 비용 절감 (5~30%)의 효율성을 갖는다. 본 시스템의 평균 접속 및 응답 시간 측정결과 값도 약 7.082초 이내로서 성능 대비 효율성이 높은 것으로 평가된다.

▸ Keyword : 인증, 비밀성, 무결성, 가용성, 접근제어

Abstract

Existing wire based physical security system solutions show limitations in time and space. In order to solve these deficiencies, a remote physical security system has been implemented using smart phone based on mobile cloud computing technique. The security functions of mobile cloud computing technique include mobile device user authentication, confidentiality of communication, integrity of information, availability of system, and target system access control, authority management and secure hand off etc. Proposed system has been constructed as remote building management system using smart phone, and also has been efficient to reduce energy cost (5~30%), result of system average access and response time 7.082 second. This systems are evaluated to have high efficiency compared to performance.

▸ Keyword : Authentication, Confidentiality, Integrity, Availability, Access Control

---

• 제1저자 : 이문구
• 투고일 : 2010. 11. 09, 심사일 : 2010. 11. 23, 게재확정일 : 2010. 12. 02.
* 김포대학 IT학부 인터넷정보과 (Dept. of Internet Information, Kimpo College)
※ 이 논문은 2010학년도 김포대학의 연구비 지원에 의하여 연구되었음.

Ⅰ. 서 론

기존의 유선상의 물리적 보안 관리 시스템은 유선관리를 위한 도구만으로 모니터링이 가능하며, 지역과 시간의 제한으로 수동적인 운영관리라는 제약 때문에 상주인력의 투입문제와 실시간 장애 통보 및 대응체계가 미흡하다[1][10]. 이러한 문제점들을 해결하고자 본 연구는 스마트폰을 이용하여 이동 중에도 원격 건물의 제반 시스템에 대한 원격 물리적 보안 시스템을 구현하였다. 구현한 "스마트폰을 이용한 원격 물리적 보안 시스템"은 건물관리 부분에서 가장 기본적인 안전 확보를 위하여 시스템 사용자의 인증기능 및 출입통제를 위한 보안 그리고 사무환경의 이상 유무 등 건물 내부의 전반적인 보안자료에 대한 접근통제 기능이 이루어지도록 하였다. 제안하는 시스템은 모바일 클라우드 컴퓨팅 기술 기반에서 요구되는 사용자 인증, 통신의 비밀성, 정보의 무결성, 시스템의 가용성, 사용자의 접근제어 및 권한 관리 그리고 안전한 핸드오프 등의 보안 기술을 구현하였다. 또한 운전관리 및 운영데이터 통합관리 등을 제공하여 시설관리 업무에 대한 통합 관리 서비스를 제공함으로써 에너지 절감, 장애 발생 시 신속한 문제인지 및 해결 방법 제시 등의 효율성 향상되며, 체계적인 관리 서비스를 제공한다.

본 논문의 구성은 다음과 같다. 2장에서는 제안하는 스마트폰을 이용한 원격 물리적 보안 시스템의 구성과 모바일 클라우드 컴퓨팅 기술 및 보안 이슈에 대하여 기술하고, 3장에서는 제안하는 시스템의 인증알고리즘과 보안 기술 방법 등을 기술하였으며, 4장에서는 시스템의 구현결과와 성능평가결과를 제시하였다. 그리고 마지막으로 5장에서는 결론과 차후 연구방향 등을 기술하였다.

Ⅱ. 시스템의 구성과 클라우드컴퓨팅보안

2.1 시스템의 구성과 클라우드컴퓨팅의 보안이슈

2.1.1 제안하는 시스템의 구성

제안하는 원격 건물관리 시스템의 구성은 [그림 1]과 같다. SNAP PAC 제어(controller)시스템을 이용하여 건물 내에 설치된 센서와 설비로부터 정보를 수집하고 이를 데이터베이스(Database)에 저장하게 되며, 인터넷 및 스마트폰(PDA 포함) 화면에서 해당 정보를 실시간 모니터링 및 제어가 가능하도록 한다[3][7].

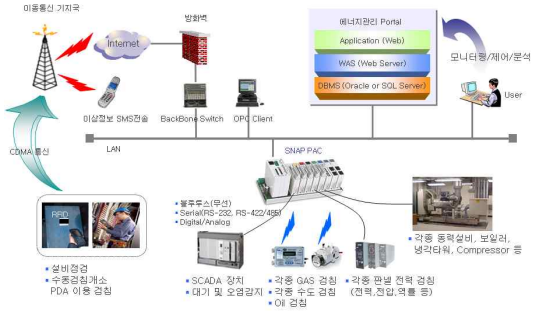

그림 1. 원격 건물관리 시스템의 구성
Fig. 1. Configuration of Remote Building Management System

2.1.2 모바일 클라우드 컴퓨팅 기술

클라우드 컴퓨팅이란 '인터넷 기술을 활용하여 IT 자원을 서비스로 제공하는 컴퓨팅'으로 정의할 수 있으며, 주요 특징은 IT 자원(소프트웨어, 스토리지, 서버, 네트워크)을 필요한 만큼 빌려서 사용하고, 서비스 부하에 따라서 실시간 확장성을 지원받으며, 사용한 만큼의 비용을 지불하는 것이다[5].

모바일 클라우드 내에는 크게 미디어 제공을 위한 데이터 스토리지 서버와 서비스를 처리하는 데이터 프로세싱 서버로 구성된다. 모바일 단말기 내에 내장되는 많은 응용 소프트웨어들은 혼자만이 동작되는 단순 응용 프로그램이 아닌 모바일 클라우드 내에 있는 서버들의 지원을 받아 원하는 서비스를 지원받는 형태 등으로 진화하고 있다. 즉, 모바일 단말기 내의 저장 공간과 처리 기능을 활용하여 일부 기능은 수행하고, 모바일 클라우드 내의 서버들로부터의 추가적인 기능을 지원받아 서비스가 이루어진다. 미래의 모바일 클라우드 컴퓨팅은 모바일 단말기의 저장 공간과 처리 능력을 확장하여 주면서 언제, 어디서든지 필요한 데이터와 콘텐츠 등의 접근을 허용하고 지원하는 유니버설 프로세싱 기능을 지원하는 환경을 제공할 것으로 예상된다[8].

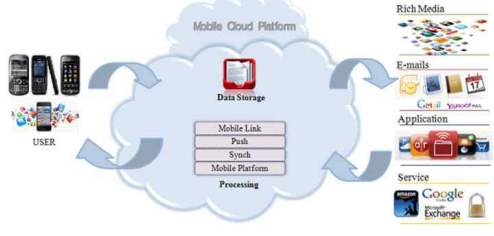

그림 2. 모바일 클라우드의 구성도
Fig. 2. Configuration of Mobile Cloud

2.1.3 모바일 클라우드 컴퓨팅 기술의 보안 요구사항

모바일 클라우드 컴퓨팅은 IT 자원을 소유하지 않고 일부 또는 모두를 아웃소싱 하는 형태이므로 필적으로 보안 문제가 발생할 수밖에 없다[6].

표 1. 모바일 클라우드 컴퓨팅 환경의 보안요구사항
Table 1. Security Requirement of Mobile Cloud Computing Environment

보안 요구사항		추가 고려 사항
기존 필수 보안 요구 사항	인증	- 상호인증 - 동적인 키 사용 - 무선구간 키 교환기반 제공 - 장치 독립적인 사용자 인증 - PKI 오버헤드 감소 - 집중형 인증/잠금 방법
	비밀성	- 키 관리기법 - 이동형/서버 장치 내 데이터 암호화 - 서버 장치에 저장된 정보 암호화 - 저 전력 암호 알고리즘
	무결성	- 모바일 특성에 맞는 무결성 보장을 위한 암호화 기법
추가적 보안 요구 사항	가용성	- DoS 공격 - 서비스 액세스 우선순위 - 대가지불 서비스
	권한 관리	- 개체 식별과 검증 - 사용자 정보 접근 제어
	익명성	- 익명성에 대한 사용자의 신탁 권한
	안전한 로밍	- 동일한 서비스 네트워크 애의 안전한 핸드오프 - 글로벌 로밍 서비스 - 핸드오프 과정에서 보안 접속 유지 및 컨텍스트 정의 및 관리 - 보안 인증 및 실시간 패킷 과금에 대한 문제

III. 제안하는 시스템의 보안기술

3.1 제안하는 시스템의 사용자 인증기술

제안하는 스마트폰을 이용한 원격 물리적 보안 시스템은 모바일 클라우드 컴퓨팅 기술 기반에서 인증 (Authentication), 비밀성(Confidentiality), 무결성(Integrity), 가용성(Availability), 권한 관리, 안전한 핸드오프 등의 보안기술이 요구된다[4].

모바일 클라우드 컴퓨팅 환경에서는 동기화를 수행하는 모바일기기, 단말의 분실 및 도난, Rogue 액세스 포인트 등을 방지하기 위해서 인증 서비스가 반드시 필요하다. 기존의 인증은 공개키 암호시스템 기반으로 신뢰기관에 의해 발급된 공개키 인증서를 바탕으로 인증하고자 하는 개체의 서명 검증 과정을 통해 이루어지고 있다. 기존의 커버로스(Kerberos) 인증 프로토콜은 양호한 네트워크 연결 상태에서 공개키 인증 방식을 통하여 인증하는 방법으로, 모바일 클라우드 컴퓨팅 환경에서는 일시적이고 불안정한 네트워크 연결 상태에서도 인증이 가능해야 한다. 그러므로 기존의 커버로스(Kerberos) 인증 방법은 모바일 컴퓨팅 사용자 인증방법으로 적절하지 않다.

모바일 클라우드 컴퓨팅 환경에서 인증을 보장하기 위해서는 상호인증, 동적 키 사용, 무선 구간 키 교환기법, 장치 독립적인 사용자 인증 방법, PKI 오버헤드 감소 등과 같은 기능이 요구되고 있다. 특히, 독립적인 사용자 인증은 단말기를 분실하거나 도난당했을 경우, 또는 여러 사용자가 공동으로 사용하는 경우에는 반드시 필요한 기능이며, 이러한 사용자 인증 방법으로는 PIN, 코드, 패스워드, 생체인식, 스마트카드 등을 추가로 도입할 수 있다[9].

3.1.1 사용자 인증 과정

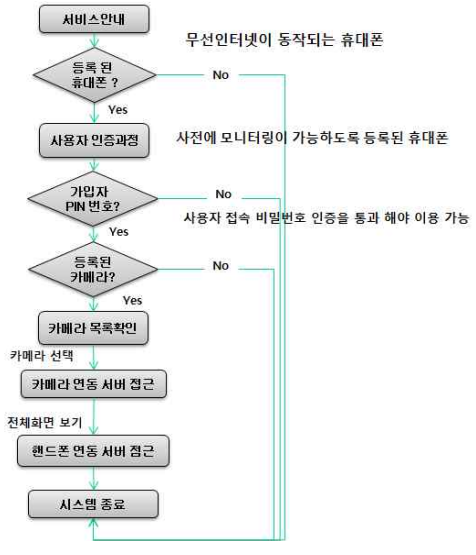

그림 3. 사용자 인증과정
Fig. 3. Process of User Authentication

본 논문에서 제안하는 사용자 인증방법은 [그림 3]과 같이 연동하는 휴대폰이 등록된 장비인지를 먼저 체크하고, 다음은 사전에 모니터링이 가능하도록 등록된 휴대폰인지를 판별하기 위해서 스마트카드를 이용한 시간 동기화(time synchronous) 기법의 일회용 PIN을 사용하였다.

여기서 시간 동기화(time synchronous) 기법의 일회용

PIN기술은 시간 기반 패스워드(Time-based Passwords) 기술인 일회용 패스워드의 특별한 형태로, 시스템과 사용자의 인증 장치의 알고리즘이 시간에 따라 변경된다. 이러한 인증 장치는 단말기에 부착된 스마트카드라고 불리 우며 현재의 패스워드를 판독한다.

사용자는 시스템 시계로부터 초기값(일종의 seed 값)을 추출하여 사용자 패스워드와 추출한 seed 값을 일회용 패스워드 생성 알고리즘 함수 F(seed)에 전달하여 일회용 패스워드(OTP)를 생성한다. 사용자는 사용자 식별 번호(PIN)와 생성된 일회용 패스워드(OTP)를 응답값(response)으로서 서버 호스트에게 전송한다. 서버 호스트는 데이터베이스로부터 수신한 사용자 식별 번호(PIN)에 해당하는 사용자 패스워드를 획득하고 사용자와 동기화되어 있는 시스템 시계로부터 seed 값을 추출하여 F(seed) 함수를 통해 일회용 패스워드(OTP)를 생성한 후 수신한 일회용 패스워드와 비교하여 일치할 경우 사용자를 인증한다. 인증 관리에서 패스워드 오류 및 로그인 실패 시 단말기 내부 데이터 삭제 기능을 제공하며, 데이터 보호 기능으로 단말기, 이동형 메모리에 대한 선택적인 데이터 암호화 기능을 제공하고 장치 방화벽 관리를 위해 wi-fi, 블루투스의 데이터 통신 인터페이스 제어 및 카메라와 이동형 매체의 제어 기능을 제공하도록 하였다 .

3.1.2 사용자 인증 알고리즘과 의사코드(Pseudo Code)

스마트폰을 이용한 원격 물리적 보안 시스템을 구현하는데 있어서 스마트폰의 구현이 iPhone 또는 Android 운영체제를 기반으로 구동되며, 다음은 iPhone기반의 알고리즘이다.

가. iPhone 알고리즘과 의사코드

a. 사용자의 PIN 을 기반으로 하는 사용자 인증기술
b. 소켓 통신연결 기술
c. 데이터 송신
d. XML 데이터 수신
e. 데이터 파싱
f. 스마트폰에 정보 제시

```
1.아이디, 비밀번호 입력
//송신 데이타 생성
NSString *sendMsg = [NSString stringWithFormat:@"<Login><id>%@</id><pw>%@</pw></Login>", idTF.text, pwTF.text];
2.소켓 통신 연결
- (void) connect:(NSString *)ip port:(int)port {
host = CFStringCreateWithCString(kCFAllocatorDefault, [ip UTF8String], NSUnicodeStringEncoding);
CFReadStreamRef readStream = NULL;
CFWriteStreamRef writeStream = NULL;

CFStreamCreatePairWithSocketToHost(kCFAllocatorDefault, host, port, &readStream, &writeStream);
instream = (NSStream*)readStream;
[instream retain];
outstream = (NSStream*)writeStream;
[outstream retain];
[instream setDelegate:self];
[instream scheduleInRunLoop:[NSRunLoop currentRunLoop] forMode:NSRunLoopCommonModes];
[instream open];
[outstream open];
CFRelease(readStream);
CFRelease(writeStream);
}
3.데이타 송신
- (void)send:(NSString *)sendMsg {
if ([outstream streamStatus] == NSStreamStatusOpen || [outstream streamStatus] == NSStreamStatusReading || [outstream streamStatus] == NSStreamStatusWriting) {
[outstream write:(const uint8_t *)[sendMsg UTF8String] maxLength:(NSUInteger)[sendMsg lengthOfBytesUsingEncoding:NSUTF8StringEncoding]];
}
}
//NSStream Delegate Method
- (void)stream:(NSStream *)aStream handleEvent:(NSStreamEvent)eventCode {
switch(eventCode) {
case NSStreamEventOpenCompleted:
[self OnOpened];
break;
case NSStreamEventHasBytesAvailable:
[self OnHasRead];
break;
case NSStreamEventHasSpaceAvailable:
[self OnHasWrite];
break;
case NSStreamEventErrorOccurred:
[self OnError];
break;
case NSStreamEventEndEncountered:
[self OnEOF];
break;
default:
NSLog(@"unknown NSStreamEvent %i", eventCode);
break;
}
}
```

그림 4. iPhone 의사코드
Fig 4. Pseudo Code of iPhone

나. Android 알고리즘

다음은 Android기반의 알고리즘이다.

a. 안드로이드 레이아웃(layout)에서 로그인/passwd) 입력 받는다.
b. XML TCP 통신으로 서버와 통신한다.

c. 로그인 id/pwd를 체크한다.
f. XML 파싱하여 화면에 뿌려준다.
d. 센서 상태 정보를 요청한다.
e. XML TCP 통신으로 서버와 통신한다.

3.2. 제안하는 시스템의 접근제어와 보안 기술

비밀성(Confidentiality)은 단말기의 분실, 도난, IP 도청(Sniffing), 동기화 등에 의해 침해될 수 있으며, 비밀성 유지를 위해서 트래픽 데이터 암호화, 키 관리기법 제공, 단말기의 중요정보 암호화, 서버 저장 데이터 암호화, 저 전력 암호화 알고리즘 등이 요구되고 있다. 특히, 모바일 컴퓨팅 환경에서는 에너지의 사용량이 중요한 고려사항으로서, 소형화, 저 전력화에 기인하여 빠르고 계산능력이 뛰어난 프로세서를 사용하는데 제약사항이 따르고 있다. 저속, 저 전력 프로세서들은 공개키 암호화 알고리즘을 사용하기에는 적합하지 않으며, 모바일 컴퓨팅 환경에 적용하기 위해서는 연산량이 많은 공개키 알고리즘의 사용 횟수를 줄이거나, 사전 계산 방법 등을 이용하여 비밀성을 제공해야 한다.

단말 분실 및 절도, 악성 프로그램 등에 의해서 단말기의 무결성(Integrity)이 침해 될 수 있다. 즉, 하나의 개체에서 다른 개체로 가는 메시지가 제 3 의 악의적인 개체에 의해 방해 받을 수 있기 때문에, 상대방과 통신 시 내용이 변경되지 않는 원본 메시지임을 보장해야 한다. 인증 및 키 교환 과정을 알고 있다면, 메시지 인증 코드(MAC)와 같은 암호 기법으로 무결성을 보장할 수 있다. 메시지 인증 코드(MAC)는 키를 사용하는 해쉬 함수로서 메시지의 인증에 주로 사용되며 압축(compression), 연산의 용이함(easy of computation)의 성질을 만족하며 추가로 '키를 모르는 공격자가 임의의 메시지에 메시지 인증 코드(MAC)값을 위장하는 것은 불가능하다(computation-resistance).'라는 특징을 가지고 있다[2].

가용성(Availability)은 DoS 공격, 악성 프로그램, 신호 방해 공격, 배터리 소진 공격 등에 의해 침해받을 수 있다. 무선 시스템에 대한 고전적인 공격이 통신 채널에 혼선을 유발하기 때문에, 모바일 컴퓨팅 환경 역시 일종의 무선 시스템이며, 이러한 통신 채널에 혼선이 야기되었을 시, 가용성이 침해당할 수 있다. 인증기법만으로는 DoS(Denial of Service) 공격을 막기 어려운 실정이며, 서비스 요구자에게 반복적으로 신원확인 요청을 할 수 있으나, 서비스 요구자의 정보는 쉽게 속일 수 있으며, DDoS(Distributed Denial of Service) 공격으로 쉽게 공격당할 수 있다.

여러 사용자가 자원을 공유하기 때문에, 공유된 데이터에 대한 접근제어가 필요하다. 사용자 권한에 따라 자원을 사용하는 것에 대한 등급 등이 있을 수 있으므로, 서비스 관리자들은 접속자들의 정보를 식별하고 검증하는 객체 식별과 인증이 필수적으로 요구된다.

모바일 환경에서는 이동통신망을 이용하여 접근 시 안전한 핸드오프 기술이 고려되어야 한다. 안전한 핸드오프는 사용자 인증, 키 관리정책, 암호화 알고리즘 협상, 그리고 권한 정책을 포괄적으로 고려하여 구현되어야 한다. 액세스 포인트 사이를 이동할 때 핸드오프 보안이 제공되어야 하며, 핸드오프 과정에서 보안 접속 유지와 데이터 보안 및 관리 등이 고려되어야 한다.

3.2.1 강제적 접근제어

제안하는 시스템은 공유된 데이터에 대한 접근제어가 필요하다. 그러므로 사용자 권한에 따라 자원을 사용하는 것에 대한 등급을 보안정책에 준하여 설정 하고 이에 접근제어 메커니즘을 적용한다. 제안하는 시스템의 강제적 접근제어는 주체 및 객체의 등급에 따라서 접근에 대한 권한을 얻도록 한다[11].
다음은 강제적 접근제어 알고리즘이다.
㈎ 강제적 접근제어 관련 DB에 연결한다.
㈏ DB로부터 데이터를 읽어온다.
㈐ DB를 닫는다.
㈑ 스마트폰 사용자의 등급과 목적지 서버 호스트 등급을 비교한 후 스마트폰 사용자의 등급이 목적지 호스트의 등급보다 작을 경우 감사기록을 남기고 접속을 일차 제안한다.
㈒ 스마트폰 사용자의 등급과 목적지 서버 호스트 등급을 비교한 후 스마트폰 사용자의 등급이 목적지 호스트 등급보다 작을 경우 감사 기록을 남기고 접속을 2단계로 제안한다.
㈓ 모두 통과하였을 경우 임의적 접근제어를 적용한다.
다음 [그림 5]는 강제적 접근제어의 흐름도이다.

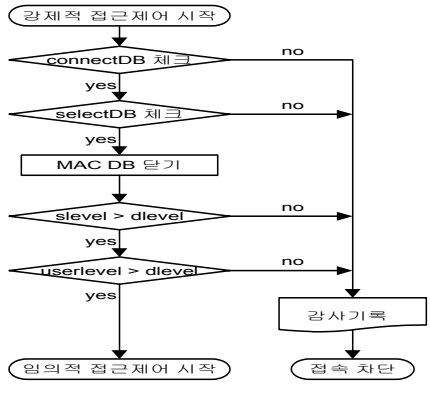

그림 5. 강제적 접근제어 흐름도
Fig 5. Flowchart of Mandatory Access Control

3.2.2 임의적 접근제어

임의적 접근제어(DAC : Discretionary Access Control)는 주체의 신분에 근거한 보안 메카니즘으로서, 주체에 대한 접근권한을 확인하여 객체에 대한 접근제어를 수행한다. 임의적 접근제어를 적용하기 위해서는 임의적 접근제어의 대상이 되는 주체 및 객체의 정의와 접근제어 규칙이 기술되어야 한다.

[그림 6]은 임의적 접근제어 처리의 설계를 위한 세부적인 흐름도를 나타낸다. 임의적 접근제어는 객체에 대한 소유권자에게 접근권한을 부여하는 방식으로 알고리즘은 다음과 같다.

㈎ 접근결정모듈에서 접근제어 데이터베이스에 사용자의 신분을 확인하기 위한 질의를 한다.

㈏ 접근제어 데이터베이스에서 사용자의 그룹, 근원지 주소, 목적지 주소를 가져오면 임의적 접근제어과정을 마치게 된다.

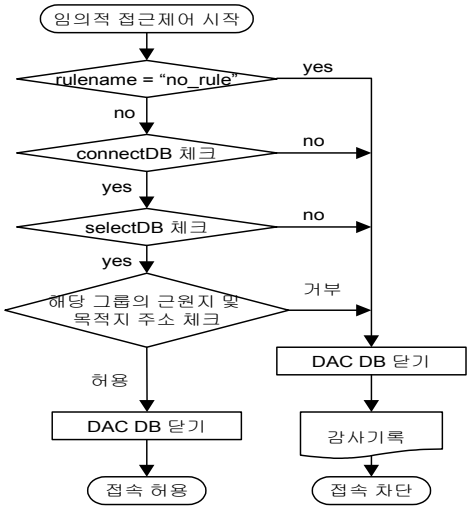

그림 6. 임의적 접근제어 흐름도
Fig 6. Flowchart of Discretionary Access Control

3.3 제안하는 시스템의 경고메시지 전송

다음 [그림 7]과 같이 원격지 건물에 설치되어 있는 서비스장비로 원격 출입문 관리, 화재감지, 온도 및 습도 체크, 냉, 난방기 설비관리, 조명관리, 원격에서 전기, 가스, 수도 검침 그리고 설치된 CCTV 등의 상황들에 대하여 정보를 모니터링 하거나 자동제어 및 필요시 원격 수동제어 정보를 인터넷 웹 포탈 또는 스마트 폰으로 정보를 전송해 줄 수 있으며, 이상의 정보를 정보 모니터링과 자동제어에 의해서 고객서비스 센터를 거쳐 이상 정보 발생 시 담당자에게 경고 및 SMS를 전송 하게 된다.

그림 7. 스마트폰을 이용한 원격 건물관리 시스템구성
Fig 7. Configuration of Remote Building Management System Using Smart Phone

IV. 구현결과와 성능평가

4.1 구현결과와 성능평가

다음 [그림 8]은 제안하는 시스템을 스마트 폰으로 서비스가 제공되는 메인화면과 출입문 정보 조회 화면이다.

그림 8. 스마트폰의 서비스
Fig 8. Service of Smart Phone

다음 [표 2]는 제안하는 스마트폰을 이용한 원격 물리적 보안 시스템에서 제공되는 보안기능과 유사한 타 업체에서 개발한 시스템의 보안기능을 비교한 자료이다. 제안하는 시스템의 보안 기능이 적용되는 단말기는 스마트폰은 물론 노트북으로 웹상의 정보도 동시에 제공할 수 있으며, 무선단말기(PDA)로도 서비스가 가능하도록 구현하였다. 서버와 통신하면서 네트워크에 연결과 상관없이 보안 정책으로 접근제어, 데이터 암호 및 인증 서비스를 제공한다. 암호화 관련된 기능으로는 연결 또는 비연결 모드에서의 이동형 보안 정책 집행,

이동단말에 대한 정책 기반의 지능형 데이터 암호화를 제공하며, 모바일단말기기에 데이터 저장 시 자동적인 데이터 암호 기능을 제공한다. 또한 단말기 분실, 도난 시 장비를 습득한 자에 의하여 물리적으로 기기가 분해되고, 데이터가 추출될 위험을 방지하기 위해서 사용자가 단말기기를 파워 오프 시 단말기 내의 데이터는 암호화 되며, 사용자가 단말기기 활성화 시에는 자동으로 데이터를 복호화 한다. 또한 물리적으로 분해되어 메모리 영역의 데이터에 직접적으로 접근 시 단말은 자동으로 잠금 상태로 전화되도록 하였다.

표 2. 제안한 시스템과 타업체 시스템 보안기능
Table 2. Access & Response time Test Result

업체 / 보안기능	제안하는 시스템	C사	U사	P사
적용 단말기	스마트폰, 노트북, PDA	스마트폰, 노트북, PDA	스마트폰, 노트북, PDA	스마트폰, 노트북, PDA
사용자 인증기능	사용자 인증기능	사용자 인증기능	사용자 인증기능	사용자 인증기능
모바일 단말기 데이터 저장	선택적인 데이터 암호화	자동적인 암호화	자동적인 암호화	선택적인 데이터암호화
인증 기능 실패	암호 데이터 삭제, 리셋	암호데이터 삭제, 리셋	-	-
동기화 과정	상호인증	상호인증	상호인증	상호 인증
단말기 분실 시 보안기능	단말기 파워 오프 시 단말기 내의 데이터는 암호화, 단말기 활성화 복호화	자동적인 fail-safe (인증 기능에 실패 시 암호 데이터 삭제 및 리셋)	단말기 암호화 및 복호화 기능제공	단말기 내부 데이터 삭제
접근제어	접근제어 기능 제공	접근제어 기능 제공	-	접근제어 기능 제공

제안하는 시스템으로 건물관리를 구현한 결과 계측, 감시, 제어를 통한 에너지 비용이 [그림 9]와 같이 최소 5에서 최대 30%까지 절감하였다.

그림 9. 실시간 전력 사용량
Fig 9. Real Time electric power consumption

제안하는 시스템이 스마트폰에서 원격 대상 서버까지 접속하여 응답 서비스를 제공하는데 기본 소요시간을 측정한 결과 [표 3]과 같이 평균 7.802초가 소요되어 전체 시스템 운용에 대한 사용자의 접근성이 좋으며, 비교적 안정적으로 서비스가 진행되었다.

표 3. 접속시간과 응답 시간 측정결과
Table 3. Access & Response time Test Result

단위 : 초

측정 항목 / 횟수	스마트폰 -> 제어서버	제어서버 -> 대상서버	대상서버 -> 제어서버	제어서버 -> 스마트폰	총 소요 시간
1	2.210	2.210	2.489	2.078	8.987
2	1.484	1.895	2.002	1.585	6.966
3	2.132	2.213	2.043	2.312	8.700
4	1.975	2.395	2.024	1.689	8.083
5	2.023	2.014	2.193	2.003	8.233
6	1.250	1.250	1.934	1.220	5.654
7	2.317	2.014	1.980	2.334	8.645
8	1.834	1.894	1.963	1.821	7.512
9	1.636	1.654	2.007	1.721	7.018
10	2.132	2.045	2.033	2.011	8.221
평균	1.899	1.958	2.067	1.877	7.802

V. 결론

본 논문은 스마트폰을 이용한 원격 물리적 보안 시스템을 모바일 클라우드 컴퓨팅 기술 기반에서 구현하였다. 모바일 클라우드 컴퓨팅은 IT 자원을 소유하지 않고 일부 또는 모두를 아웃소싱 하는 형태이며, 모바일 클라우드 컴퓨팅 시스템 도입에 따라 업무의 실시간화를 통하여 자원 절감 및 효율화를 극대화하며, 생산성을 증대할 수 있으며, 스토리지 클라우

드와 지속적인 업무자료 동기화를 통해 업무정보 관리 자동화로 비용을 절감할 수 있고, 불필요한 업무를 줄일 수 있다.

뿐만 아니라 제안하는 시스템은 건물관리 부분에서 가장 기본적인 안전 확보 및 출입통제를 위한 보안 그리고 사무환경의 이상 유무 등 건물 내부의 전반적인 보안문제에 대한 데이터베이스 구축이 이루어지도록 하였으며, 모바일 클라우드 컴퓨팅 기술 기반에서 요구되는 인증, 비밀성, 무결성, 그리고 가용성, 권한 관리, 안전한 핸드오프 등의 보안요구 사항들을 설계함으로써 기존의 건물관리와 클라우딩 컴퓨팅 환경이 갖는 보안 문제 등을 해결하였다. 그리고 장애 발생 시 신속한 문제 인지와 해결 방법 제시 등의 체계적인 관리 서비스를 제공하도록 구현하였다.

시스템의 구현결과 계측, 감시, 제어를 통한 에너지 비용 이 최소 5에서 최대 30%까지 절감되었으며, 본 시스템의 구현으로 검침시간의 절감, 데이터의 정합성과 신뢰성을 보장할 수 있고, 장애 발생 시 신속한 문제 인지와 해결 그리고 통합적 운영에 따른 업무 협조 및 정보교환 등의 효과적인 수행 그리고 정확한 원가산정을 위한 기초 데이터 제공 전체 비용대비 시스템의 효율성이 높은 것으로 평가되었다. 보안기능으로 사용자 인증과 접근제어 기술로 시스템에 접속하고 응답하는데 소요되는 시간은 평균 10초 이내의 비교적 안정적인 서비스제공이 이루어졌다. 차후 연구에서는 모바일 단말기의 저장 공간과 처리 능력을 확장하여 언제, 어디서든지 필요한 데이터와 콘텐츠 등의 접근을 허용하고 지원하는 서비스 환경을 제공할 수 있도록 하고, 현재는 모바일 단말기 데이터 저장을 사용자의 선택에 의해 암호화를 시행하였으나, 자동적인 암호화체계를 구축하기 위한 알고리즘을 제안하도록 연구를 지속할 할 것이다.

참고문헌

[1] Sumei Dai , Zhiying Song , Ruiqing Jia, “Web Based Fluid Mechanics Experimental System” 2010 International Conference on Electrical and Control Engineering, pp. 3134-3137, June 2010.

[2] A. Holopainen , F. Galbiati , K. Voutilainen, "Use of Smart Phone Technologies to Offer Easy-to-Use and Cost-Effective Telemedicine Services", First International Conference on the Digital Society (ICDS'07) pp. 4, Jan. 2007.

[3] Daniel Brooker , Thomas Carey , Ian Warren “Middleware for Social Networking on Mobile Devices” IEEE Computer Security. pp. 202-211, April 2010.

[4] Eiman Kanjo , Jean Bacon , David Roberts , Peter Landshoff, "Making Smart Phones Smarter", IEEE Computer Security. pp. 50-57 Oct. 2009.

[5] Yi Wei , M. Brian Blake, "Service-Oriented Computing and Cloud Computing: Challenges and Opportunities" IEEE Internet Computing, pp. 72-75, Nov. 2010.

[6] Qian Wang , Cong Wang , Kui Ren , Wenjing Lou , Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems, Oct. 2010.

[7] Nichols, J. Myers, B.A. Sch. of Comput. Sci., Carnegie Mellon Univ., Pittsburgh, PA, Nichols, J. Myers, B.A. "Controlling Home and Office Appliances with Smart Phones" Pervasive Computing, IEEE , 2006 , Page(s): 60 - 67

[8] Liang-Jie Zhang , Jia Zhang , Jinan Fiaidhi , J. Morris Chang, “Hot Topics in Cloud Computing”, IT Professional, pp. 17-19, Sept. 2010.

[9] Thomas Weigold , Thorsten Kramp , Michael Baentsch, "Remote Client Authentication" IEEE Security and Privacy, pp. 36-43, July 2008.

[10] Yongxiang Bai , Youhua Hou , Dazhong Fang , Xuwei He , Changsheng Zhu, "A Remote Real-Time On-line Monitoring and Control System for Large-Scale Wind Farms" IEEE Security and Privacy, pp. 3220-3223, June 2010.

저 자 소 개

이 문 구

1984 : 숭실대학교 전자계산학 학사
1993 : 이화대학교 대학원 전산교육학석사
2000년 : 숭실대학교 대학원 컴퓨터학박사
2000 -현재 : 김포대학 IT학부
인터넷정보과 부교수
관심분야 : 암호알고리즘, 인터넷보안, 시스템 보안
E-mail : yeon0330@kimpo.ac.kr