Regular paper

Journal of the KIECS. pp. 369-376, vol. 13, no. 2, Apr. 30 2018, t. 88, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2018.13.2.369

안드로이드 기반 산업용 가스터빈 원격 모니터링 시스템 구현

최준혁* · 이동익**

Android-based Implementation of Remote Monitoring System for Industrial Gas Turbines

Joon-Hyuck Choi* · Dong-Ik Lee**

요 약

본 논문은 안드로이드 기반으로 구현된 실시간 원격 모니터링 시스템을 제안한다. 원격 모니터링 기술은 모니터링에 필요한 비용의 절감과 비정상 상태의 빠른 발견에 이점이 있다. 제안된 모니터링 시스템은 민감한 정보를 보호하기 위해 RSA(Rivest Shamir Adleman) 알고리즘을 이용하는 보안 통신을 사용한다. 가스터빈의 이상 상황이 발생하였을 때, 원격 모니터링 시스템은 사용자의 주의를 끌기 위해 푸시 메시지를 이용한 경고를 한다. 제안된 시스템은 가상 데이터 발생기를 포함하는 실험 환경에서의 실험으로 검증되었다.

ABSTRACT

This paper presents an android-based implementation of real-time remote monitoring system for industrial gas turbines. The use of remote monitoring techniques can be beneficial in terms of not only the reduction of monitoring cost but also the earlier detection of abnormal status. In order to achieve the ability of protecting sensitive information from unauthorized persons, the proposed system supports secure transmissions using the RSA(Rivest Shamir Adleman) algorithm. In the event of abnormal situation on the gas turbine, the remote monitoring system generates an alarm to attract the user's attention by exploiting a push-message technique. The proposed system has been verified through a series of experiments with an experimental setup including a virtual data generator.

키워드

Android, Monitoring System, Gas Turbine, Security, RSA Algorithm
안드로이드, 모니터링 시스템, 가스 터빈, 보안, RSA 알고리즘

Ⅰ. 서 론

발전 시설은 국가 산업 및 국민 삶의 기반이 되므로 높은 수준의 안정성이 요구된다. 체르노빌과 후쿠시마 원자력 발전소 사고 사례에서 볼 수 있는 것처럼 발전 시설의 오작동에 따른 사고 발생시 막대한 경제적, 환경적 손실 뿐 아니라 인명손상까지 초래할 수 있다[1]. 발전 설비는 24시간 가동이 불가피하며, 이상 상태 발생 직후 신속한 대처가 이루어지 않으면 2차, 3차의 심각한 피해를 유발하므로, 가스 터빈 등 주요 설비에 대한 24시간 상시 모니터링이 필수적이다. 이를 위해 대부분의 발전소에서는 중앙 감시/모니

* 경북대학교 전자공학부(skyjun4@nate.com)
** 교신저자 : 경북대학교 전자공학부
· 접 수 일 : 2018. 01. 12
· 수정완료일 : 2018. 02. 27
· 게재확정일 : 2018. 04. 15
· Received : Jan. 12, 2018, Revised : Feb. 27, 2018, Accepted : Apr. 15, 2018
· Corresponding Author : Dong-Ik Lee
School of Electronics Engineering, Kyungpook National University
Email : dilee@knu.ac.kr

터링 시설을 갖추고 있으며, 관련 인력이 이 시설 내에 상주하며 24시간 모니터링을 수행하고 있다. 그러나 발전소내 중앙 감시/모니터링 시설에 상주하는 인력에만 의존하는 방식은 과도한 인건비가 소요될 뿐 아니라, 관리자의 피로누적에 따른 집중력 저하 등으로 인해 감시 업무가 소홀해질 우려가 크다. 따라서 발전소내 상주 인력 뿐 아니라 발전소 외부에서도 상시적으로 발전설비 상태를 감시할 수 있는 원격 모니터링 시스템의 필요성이 제기되고 있으며 최근 정보통신 기술이 급속하게 발전함에 따라, 사물인터넷 기술이 활용 범위가 넓어져 발전소의 모니터링 시스템에도 적용할 수 있다[2]. 그럼에도 불구하고 현재까지 발전소 원격 모니터링 시스템의 적용 사례를 찾아보기 어려운 실정인데, 이는 개인 단말기와 무선 통신을 이용하는 시스템의 데이터 보안 취약성에 기인한다[3-4].

본 논문에서는, 관리자들이 발전소 중앙 감시 시설에 상주하지 않더라도 가스 터빈의 주요 상태변수를 상시적으로 모니터링 할 수 있는 안드로이드 기반 원격 모니터 시스템을 구현한다. 제안한 시스템에서는 외부 해킹에 의한 가스 터빈 데이터의 유출 위험을 최소화할 수 있도록 3가지 기법을 복합적으로 적용한다. 즉 사용자 보안 등급에 따른 차등 권한 부여, RSA(: Rivest Shamir Adleman) 알고리즘[5]을 이용한 데이터의 암호화, 그리고 개인용 단말기에 가스 터빈 관련 데이터의 저장을 금지하는 방법을 함께 적용함으로써 효과적인 실시간 데이터 보안을 확보하고자 한다. 끝으로 가상 데이터 발생기(data generator)를 이용한 다양한 실험을 통해 제안한 원격 모니터링 시스템의 성능과 효용성을 검증한다.

II. 원격 모니터링 시스템의 주요 기능 설계 및 구현

2.1 전체 시스템 구성

일반적인 중앙 모니터링/제어 시스템과 함께 원격 모니터링 시스템을 포함하는 가스 터빈 모니터링 시스템의 구성 개념은 그림1과 같다. 본 논문에서 다루는 원격 모니터링 시스템은 그림1의 오른편에 제시된 것처럼, 발전소 내·외부의 임의 장소에 위치한 시스템 관리자(off-site operators)가 개인용 스마트 단말기를 이용하여 중앙 모니터링/제어 시스템의 데이터에 접근하고 필요시 긴급명령을 전송할 수 있는 어플리케이션 소프트웨어를 가리킨다. 따라서 원격 모니터링 시스템은 기존의 가스 터빈 상태 데이터 획득 장치(turbine status data acquisition unit) 및 중앙 모니터링/제어 시스템과 연동하여 동작하도록 설계된다.

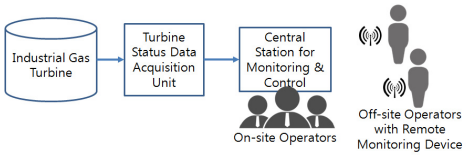

그림 1. 산업용 가스 터빈을 위한 원격 모니터링 시스템 구성 개념도
Fig. 1 Overview of remote monitoring system for industrial gas turbines

2.2 원격 모니터링 어플리케이션

최근 통계에 따르면, 2014년 기준 국내 스마트폰 보급률은 78.6%에 이른다[6]. 이 가운데 안드로이드 기반 스마트폰의 국내 시장 점유율은 77%이다[1]. 따라서 본 연구에서는 안드로이드 기반의 스마트 단말기를 이용하여 원격 모니터링 어플리케이션을 구현하였다.

제안한 원격 모니터링 어플리케이션은 Java의 소켓(socket) 통신을 이용하여 구현하였으며, 전체 구성도는 그림2와 같다. 클라이언트 장치(client device)에서 어플리케이션을 통해 로그인, 권한 정도, 데이터 정보 등을 소켓 서버(socket server)와 주고받으며, 안드로이드에서 기본적으로 제공하는 MySQL[7] 데이터베이스를 사용하여 데이터를 관리한다. Java 데이터 생성기(Java data generator)는 본 연구결과의 검증에 필요한 데이터를 제공하며, 최종 개발이 완료되면 중앙 모니터링/제어 시스템 및 가스 터빈 상태 데이터 획득 장치로부터 제공되는 데이터로 대체되도록 설계하였다.

원격 모니터링 어플리케이션은 발전소의 기존 설비(가스 터빈 상태 데이터 획득 장치 및 중앙 모니터링

1) StatCounter, http://www.statcounter.com/

/제어 시스템)와 연동되어, 관리자가 가스 터빈 상태 정보에 접근할 수 있는 기능을 제공한다. 이를 위해 그림3과 같이 원격 모니터링 어플리케이션의 주화면 및 세부화면 등 다양한 사용자 인터페이스를 구성하였다. 주화면은 관리자가 가스 터빈의 동작 상태를 쉽게 알 수 있도록 시스템 계통도 및 주요 동작값을 선택적으로 표시한다. 반면 세부화면은 각 부시스템 별 상세 동작값을 실시간으로 출력하도록 구성하였다.

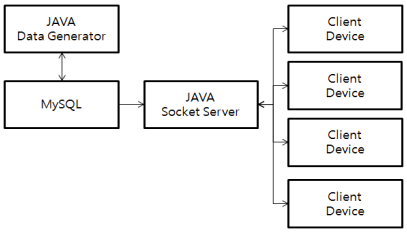

그림 2. 원격 모니터링 어플리케이션 구성도
Fig. 2 Configuration of remote monitoring application

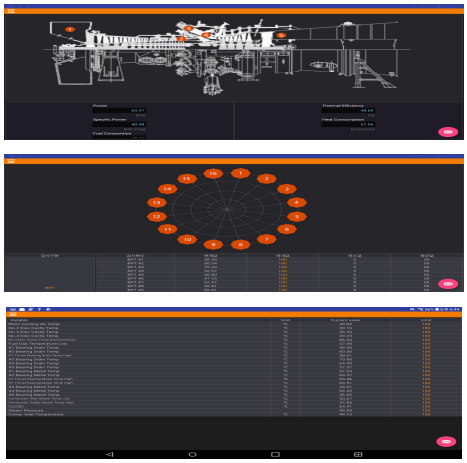

그림 3. 원격 모니터링 어플리케이션 사용자 인터페이스
Fig. 3 User interfaces for remote monitoring application

2.3 GCM기반 알림 서비스

원격 모니터링 어플리케이션의 핵심 기능은 가스 터빈에 발생한 이상 상태에 대해 시설 외부의 관리자가 신속하게 인지할 수 있도록 지원하는 것이다. 어플리케이션 사용자가 항상 원격 모니터링 시스템에 접속하여 데이터를 확인하고 있다고 볼 수는 없다. 따라서 어플리케이션의 실행 여부와 무관하게 이상 상태 발생 시 사용자에게 알림을 제공하는 기능이 필수적이다. 본 논문에서는 GCM(: Google cloud message) 기반의 푸쉬 메시지(push message)를 통해 이상 상태 발생을 알려주는 기능을 구현하였으며, 이를 위한 핵심 알고리즘은 그림4와 같다. GCM 서비스를 제어하는 서버에서 발전 시설의 이상 데이터 발생을 감지하는데, 이상 데이터가 발생할 때마다 푸쉬 메시지를 송신할 경우 중복 송신의 우려가 있다. 따라서 정상 데이터에서 이상 데이터로 변경되는 시점의 에지(edge)값을 기준으로 푸쉬 메시지를 송신하도록 설계하였다. 그림5는 데이터 값이 설정 한계치(threshold)의 95% 수준을 넘어가면 알림을 발생하도록 구현한 사례를 나타내고 있다.

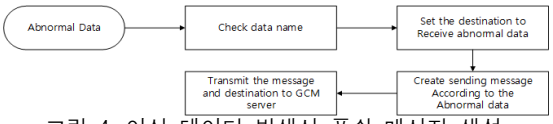

그림 4. 이상 데이터 발생시 푸쉬 메시지 생성 알고리즘
Fig. 4 Algorithm to generate a push message in case of abnormal status

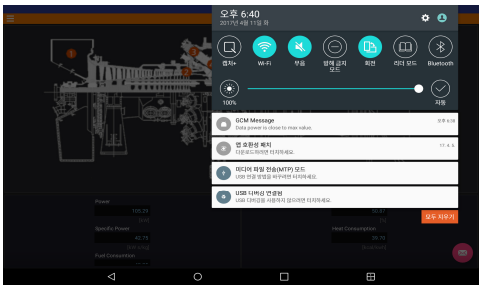

그림 5. 이상 상태 발생시 알림 기능을 보여주는 화면 사례
Fig. 5 Screenshot of push-messages to give an alarm for abnormal status

III. 원격 모니터링 시스템의 보안기법

3.1 적용 기법 개요

원격 모니터링 시스템은 개인 스마트 단말기와 무선 통신을 이용하므로, 물리적으로 악성 사용자의 침입을 제한하기 어려운 문제점이 있다. 최근 원자력 발

전소에 대한 외부 해킹 사고에서 볼 수 있는 것처럼, 가스 터빈 관련 내부 데이터가 유출될 경우 심각한 사회적, 경제적 피해를 초래할 수 있다[3]. 이러한 우려로 인해, 원격 모니터링 시스템의 많은 장점에도 불구하고 발전소에 실제 적용된 사례를 찾아보기 어려운 실정이다. 금융 시스템 등에서 데이터 암호화를 통한 보안 기술의 하나인 1024비트 RSA 알고리즘[8]이 널리 적용되고 있으나, 본 연구에서 다루는 개인용 스마트 단말기 기반의 가스 터빈 원격 모니터링에 그대로 적용하기에는 실시간 구현에 어려움이 따른다.

일반적으로 시스템공학 분야에서 다루는 고장에 따른 위험도(risk)는 고장발생 빈도와 고장에 따른 결과의 중대성에 비례하는 것으로 나타낸다[9]. 동일한 개념을 데이터 보안에 적용하면, 데이터 보안의 취약성(R)은 데이터 노출 빈도(P)와 노출된 데이터의 중요도(S)에 비례하는 것으로 가정할 수 있으며, 본 논문에서는 이러한 가정에 기초하여 실시간 처리가 가능한 보안 기법을 설계하였다.

$$R = P \times S \tag{1}$$

식(1)에 나타낸 것처럼, 데이터가 외부에 노출되는 빈도 및 해당 데이터가 포함하는 정보의 중요도가 낮을수록 데이터 유출에 따른 피해 정도가 감소한다고 볼 수 있다. 따라서 본 논문에서는 실시간 구현의 어려움이 따르는 RSA 알고리즘의 1024비트 합성수를 512비트 합성수로 대체하되, 이로 인해 커질 수 있는 보안 취약성은 데이터의 노출 빈도 최소화 및 개별 데이터의 중요도를 분산시킴으로써 보완할 수 있도록 설계하였다. 즉 데이터 노출 빈도 최소화를 위해 사용자의 보안 등급별로 데이터 접근 권한을 차등적으로 제한하였으며, 일부 데이터가 유출되더라도 이로부터 유의미한 정보를 얻을 수 없도록 개인 단말기의 가스 터빈 데이터 저장 기능을 제한하는 방법을 적용하였다.

3.2 RSA 알고리즘 설계 및 구현

RSA 알고리즘은 높은 안정성과 보안 강도로 인해 데이터 암호화 기법으로 폭넓게 적용되고 있다[5]. RSA 알고리즘의 구현을 위해 임의의 서로 다른 큰 소수 p와 q를 선택한 후, 두 소수를 곱한 합성수 n=p×q를 구한다. 그리고 합성수를 기반으로 공개키와 개인키를 생성한 후, 클라이언트의 공개키는 데이터 서버에게 공개되고, 서버는 공개키를 이용하여 데이터를 암호화한 후 클라이언트에게 전송하는 방식을 적용한다.

일반적으로 보안 전문가들은 1024비트 이상의 RSA 합성수를 이용하도록 권고하고 있다[8]. 그러나 본 논문에서 다루는 가스터빈 원격 모니터링 시스템의 경우, 개인용 스마트 디바이스를 이용한 1024비트 RSA 알고리즘의 실시간 구현에 어려움이 따른다. 따라서 본 논문에서는 원격 모니터링 시스템에서 전송되는 데이터의 암호화를 위해 512비트(155자리) RSA 합성수를 적용하고, 이로 인해 저하된 보안 강도는 다음 절에서 설명하는 노출빈도 제한과 데이터 중요도 분산을 통해 보완하였다.

RSA 알고리즘을 구현하기 위해 Java 언어를 이용하여 임의의 소수 생성 함수, 모듈러 연산 수행 함수, 공개키 생성 함수, 비밀키 생성 함수 등을 설계하였다. 상기 함수를 활용하여 암호화 및 복호화 기능을 수행하는 과정은 그림6 및 그림7에 제시하였다. 단말기는 서버에 데이터를 요청할 때 공개키와 개인키를 생성하며, 이 가운데 공개키와 데이터 요청 메시지를 서버로 전송한다. 서버에서는 수신된 공개키를 이용하여 데이터를 암호화한 후 단말기로 송신하고, 단말기에서는 개인키를 이용하여 수신 데이터를 복호화하여 출력한다.

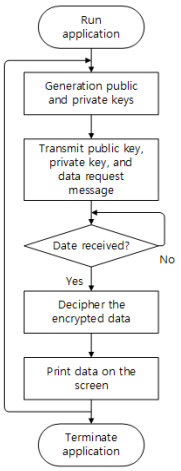

그림 6. 클라이언트 암호화 알고리즘 흐름도
Fig. 6 Flowchart of encryption algorithm for client

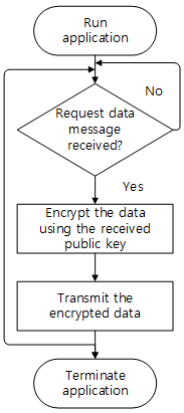

그림 7. 서버 암호화 알고리즘 흐름도
Fig. 7 Flowchart of encryption algorithm for server

3.3 512비트 RSA 알고리즘의 취약점 보완

RSA 알고리즘의 보안성 검증을 위한 시도의 일환으로서, 수 백 대의 컴퓨터를 동원하여 5개월에 걸친 시도 끝에 512비트 RSA 합성수에 대한 해독에 성공한 사례가 보고된 바 있다[8]. 이 실험의 결과에 따라 보안 전문가들은 1024비트 이상의 합성수 사용을 권장하고 있다. 그러나 앞서 언급한 바와 같이, 본 연구에서는 데이터 송신 및 수신을 실시간으로 구현하기 위해 암호화에 소요되는 시간을 줄여야 할 필요가 있기 때문에 불가피하게 512비트 합성수를 사용하여 RSA 암호화 알고리즘을 구현하였다. 따라서 이로 인해 발생하는 보안 강도 취약점을 보완하고자, 본 논문에서는 가스 터빈 모니터링 시스템의 특성을 기반으로, 주요 데이터의 노출빈도를 줄이고 개별 데이터의 중요도를 분산시키는 방법을 동시에 적용하였다.

3.3.1 보안등급별 차등 권한 부여

먼저 중요 데이터의 외부 노출빈도를 최소화할 수 있도록 원격 모니터링 어플리케이션 사용자의 보안등급에 따라 접근 가능한 데이터의 종류와 접속 지속시간을 제한하도록 설계하였다. 보안 등급별 접근 가능한 데이터의 종류는 가스 터빈의 제작사 및 발전소 운용 규정 등에 따라서 달라질 수 있다. 예들 들면, 엔진의 연료 소모량, 추력 등에 대한 정보를 확보하면 해당 엔진에 대한 성능 정보를 얻을 수 있을 뿐 아니라 역모델링이 가능해짐으로써[10], 경쟁사에 주요 정보가 유출될 위험이 있다. 따라서 위와 같은 데이터는 높은 보안등급을 가지고 있는 사용자에게만 제공된다. 반면 가스터빈의 회전수, 온도 등은 유지보수 기술자 등 낮은 보안등급을 가지고 있는 사용자에게도 제공된다.

보안등급별 차등 권한 기능의 구현은 그림8과 같으며, 실제 구현 결과 사례는 그림9에 제시하였다. 먼저 서버에서는 로그인을 요청하는 사용자의 보안등급 정보(ID)에 따라서 우선순위(priority)값을 부여하고 사용자의 어플리케이션은 부여받은 우선순위 값에 따라 UI를 구성하고 필요한 데이터를 서버에 요청한다. 서버는 해당 사용자가 요청한 데이터에 접근할 수 있는 우선순위 값을 가졌는지 확인한다. 이어서 사용자의 우선순위 값이 요청한 데이터에 접근 가능하다고 판별되면 해당하는 데이터를 송신한다. 사용자의 어플리케이션은 수신한 데이터를 앞서 구성한 UI를 통해 출력한다.

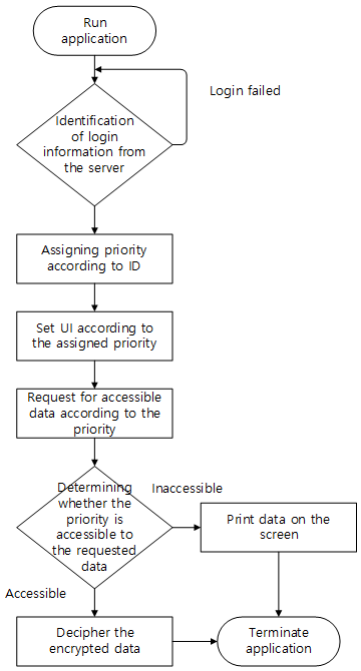

그림 8. 차등 권한 부여 알고리즘
Fig. 8 Differential authorizing algorithm

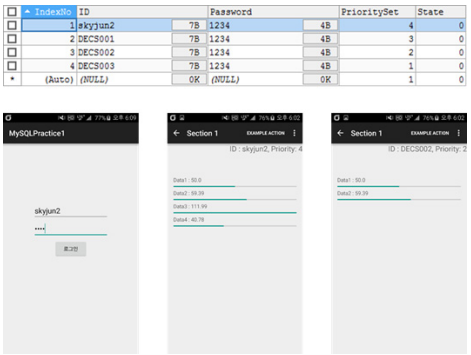

그림 9. 차등 권한 부여 기능의 구현
Fig. 9 Implementation of differential authorizing function

3.3.2 수신 데이터의 개인 단말기 저장 제한

일반적으로 모니터링 시스템에서 출력되는 짧은 순간의 데이터로부터 유의미한 가스 터빈 정보를 얻기는 어렵다. 가스 터빈의 상태에 대한 정확한 정보를 확보하기 위해서는 일정한 기간 동안의 데이터 누적과 이를 통한 상태 변수들의 변화 추세를 지속적으로 분석할 필요가 있다. 이러한 특성을 고려하여, 본 논문에서는 서버에서 전송되는 상태 모니터링 데이터를 연속적으로 화면에 출력만 가능할 뿐 개인 단말기에 과거 데이터를 저장할 수 없도록 설계하였다. 따라서 외부 해킹에 의해 가스 터빈의 상태를 파악하기 위해서는 512비트 RSA 합성수를 이용하여 암호화된 데이터를 실시간으로 연속 해독한 후 주요 변수들의 상태 변화를 추적할 때 가능하다. 그런데 앞서 언급한 512비트 합성수 해독 실험[8]에서 수 백 대의 컴퓨터와 5개월의 시간이 소요된 점을 고려하면, 512비트로 암호화된 데이터를 장시간에 걸쳐 연속적으로 실시간 해독하여 가스 터빈의 상태에 관한 유의미한 정보 획득에 성공할 확률은 매우 낮을 것으로 판단된다.

Ⅳ. 실험 및 검증

4.1 원격 모니터링 시스템 검증

본 논문에서 제시한 원격 모니터링 시스템의 검증을 위해 Java 기반의 데이터 생성장치(data generator)를 제작하였으며, 검증을 위한 실험장치의 구성은 그림10과 같다.

데이터 생성장치는 앞 서 그림1의 가스 터빈 상태 변수 획득 장치 및 중앙 모니터링/제어 시스템으로부터 제공되는 데이터를 대신하여 임의의 데이터를 생성한 후 개인 단말기로 전송한다. 이때 생성되는 데이터 A, B, … , N은 N개의 센서값 또는 상태 데이터로 가정한다. 데이터 수신부에서는 서로 다른 보안등급 ID를 가진 사용자들로 구성하며, 각 ID에 따라 데이터 접근 권한이 차별화되는지 여부를 확인하였다. 임의의 이상 상태를 나타내는 데이터를 생성하고, 알림 메시지의 수신 여부를 통해 원격 모니터링 시스템의 효용성 및 사용자 편의성을 확인하였다.

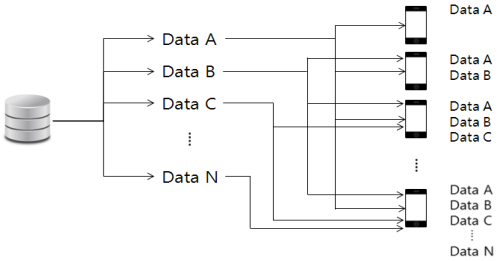

그림 10. 원격 모니터링 시스템 검증 개념도
Fig. 10 Concept for verifying remote monitoring system

4.2 보안 기법의 검증

RSA 알고리즘의 안정성은 십여 년 이상을 통해 다양한 검증이 이루어졌으므로[11-12], 본 논문에서는 개인 스마트 단말기에 적용하여 실시간 처리가 가능한 지에 대한 검증을 수행하였다. 본 실험에서는, 실시간 상태 데이터의 업데이트 주기를 0.25s~1s로 설정하고, 보안 기법의 처리시간을 측정하여 실시간 데이터 송수신에 미치는 영향을 확인하였다.

암호화 알고리즘의 전체 처리에 소요되는 시간과 하나의 데이터 처리에 소요되는 시간 각각을 Java 언어 내부 함수를 이용해 200만회 이상 반복 수행 하였다. 실험 결과는 각각 2.7ms부터 5.3ms, 18.53ms부터 30.905ms의 100개의 구간을 가지는 도수분포표를 이용해 분석되었다. 암호화 알고리즘의 하나의 데이터 처리에 소요되는 시간의 산술평균과 분산은 각각 3.08ms, 0.083이며 전체 데이터 처리에 소요되는 시간의 산술평균과 분산은 각각 22.1ms, 0.913이다. 그림 11, 그림 12는 암호화 알고리즘 수행시간의 분포를 보여준다. 실험 결과로부터 전체 데이터의 암호화 및 복호화를 위해 평균 22.1ms의 시간이 소요됨을 확인하

였다. 이는 원격 모니터링 어플리케이션의 데이터 업데이트 주기 0.25s~1s에 비해 1/12~1/50 정도의 짧은 시간이다. 따라서 데이터 송수신 소요 시간과 어플리케이션 수행 시간을 감안하더라도 제안한 보안 기법은 원격 모니터링 시스템의 실시간 데이터 처리에 적합한 것으로 판단된다.

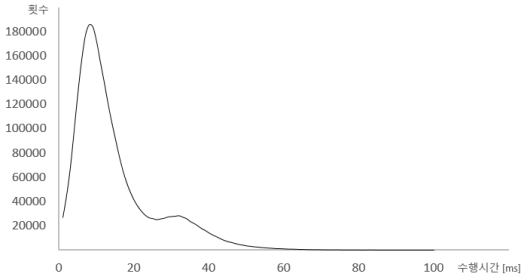

그림 11. 암호화 알고리즘의 하나의 데이터 처리 시간 분포
Fig. 11 Distribution of RSA algorithm execution time for one data

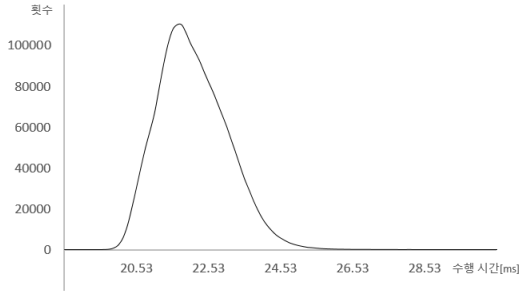

그림 12. 암호화 알고리즘의 전체 데이터 처리 시간 분포
Fig. 12 Distribution of RSA algorithm execution time for entire data

Ⅴ. 결론

본 논문에서는 24시간 운용되는 산업용 가스 터빈의 상태를 발전소 외부에서 실시간으로 감시할 수 있는 원격 모니터링 시스템을 구현하고, 실험을 통해 효용성과 타당성을 검증하였다. 제안한 시스템은 안드로이드 기반의 개인용 스마트 단말기와 무선 통신을 이용하며, 이로 인한 보안 취약성을 해결하기 위해 RSA 알고리즘을 이용한 실시간 보안 기법을 함께 적용하였다. 아울러 원격 모니터링 시스템에 접근하는 사용자의 보안등급에 따라 데이터 접근 권한을 차별화하고 수신한 데이터를 개인 단말기에 저장하지 않도록 설계함으로써 주요 데이터의 노출 빈도와 데이터 유출에 따른 위험성을 감소시킬 수 있도록 구현하였다. 본 논문에서 구현한 원격 모니터링 시스템은 기구축된 발전 설비 감시 시스템과 연동하여 상태 데이터를 제공하므로 고가의 추가 장비 또는 진단 소프트웨어를 도입하지 않더라도 24시간 모니터링을 위한 상주 인력의 감소 및 보다 안정적인 감시 효과를 기대할 수 있다.

감사의 글

이 논문은 2016년 경북대학교 연구년 교수 연구비에 의하여 연구되었음.

References

[1] J. Cho and K. Jeong, “Remote Controlled Robots Used for the Mitigation of the Fukushima Nuclear Power Plant Accident,” *J. of Institute of Control, Robotics and Systems*, vol. 2011, no. 12, 2011, pp. 148-151.

[2] X. Hao and C. Kim, “Design and Implementation of a Smart Home Cloud Control System Using Bridge based on IoT,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 12, no. 5, 2017, pp. 865-872.

[3] H. Ko and H. Kim, “A Study on Vulnerability Analysis and Incident Response Methodology based on the Penetration Test of the Power Plant’s Main Control Systems,” *J. of the Korea Institute of Information Security and Cryptology*, vol. 24, no. 2, 2014, pp. 295-310.

[4] S. Park, W. Choi, B. Chung, J. N. Kim, and J. M. Kim, “The Study on the Cyber Security Requirements of Cyber-Physical Systems for Cyber Security Frameworks,” *J. of Institute of Embedded Engineering of Korea*, vol. 7, no. 5, 2012,

pp. 255-265.
[5] T. H. Cormen, *Algorithms Unlocked.* London: MIT Press, 2013.
[6] Y. Jang, "Analysis of Concentration-Related EEG Component Due to SmartPhone," *J. of the KIECS*, vol. 11, no. 7, 2016, pp. 712-722.
[7] Y. Shin and J. Ryu, "Study on Adoption of Suitable Encryption Scheme According to Data Properties on MySQL Database," *Proc. Korea Computer Congress 2010*, Jeju island, South Korea, June, 2010.
[8] R. D. Silverman, "A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths," *Bulletin of RSA Laboratories, no. 13,* April, 2000.
[9] B. S. Dhillon, *Engineering Safety.* Singapore: World Scientific, 2003.
[10] C. Kong and L. Semyeong, "A Study of Inverse Modeling from Micro Gas Turbine Experimental Test Data," *J. of Korean Society of Propulsion Engineers*, vol. 13, no. 6, 2009, pp. 1-7.
[11] A. Selby and C. Mitchel, "Algorithms for Software Implementations of RSA," IEE *Proc. E – Computer and Digital Techniques*, vol. 136, no. 3, 1989, pp. 166 – 170.
[12] T. Fujita, K. Kogiso, K. Sawada, and S. Shin, "Security Enhancement of Networked Control Systems Using RSA Public-key Cryptosystem," *Proc. 10th Asian Control Conf.*, Kota Kinabalu, Malaysia, May, 2015.

저자 소개

최준혁(Joon-Hyuck Choi)

2015년 경북대학교 전자공학부 졸업(공학사)
2018년 경북대학교 대학원 전자공학부 졸업(공학석사)
2018년~현재 경북대학교 대학원 박사과정
※ 관심분야 : 제어공학, 임베디드 시스템

이동익(Dong-Ik Lee)

1987년 경북대학교 전자공학과 졸업(공학사)
1990년 경북대학교 대학원 전자공학과 졸업(공학석사)
2002년 University of Sheffield 졸업(공학박사)
2005년~현재 경북대학교 전가공학부 교수
※ 관심분야 : 임베디드 시스템 제어, 고장진단 및 고장복구, 고신뢰성 네트워크 기반 제어 등