Journal of the Korea Academia-Industrial cooperation Society
Vol. 18, No. 4 pp. 677-684, 2017

https://doi.org/10.5762/KAIS.2017.18.4.677
ISSN 1975-4701 / eISSN 2288-4688

산업용 자동화 장비를 위한 스마트 제어 시스템 설계

김보헌, 김황래*
공주대학교 컴퓨터공학부

A Design of the Smart Control System for Industrial Automation Equipment

Bo-Hun Kim, Hwang-Rae Kim*
Division of Computer Engineering, Kongju National University

요 약 스마트 기기는 휴대하기 편리하고 애플리케이션이 개발이 쉬운 장점으로 다양한 산업 분야에 적용되고 있다. 그러나 산업용 장비 분야에서는 장비에서 제공되는 정보에 대한 보안 문제 및 원격지에서 장비의 액추에이터를 제어할 경우 사고가 발생할 수 있다. 본 논문에서는 위 문제에 대한 해결 방법과 스마트 제어 시스템을 산업용 자동화 장비에 적용할 경우 장점에 관한 연구를 수행하였다. 이런 문제 해결을 위해 장비 조작 시 발생할 수 있는 사고에 대해 질의를 이용한 매뉴얼 조작 방법과 스마트 기기를 이용한 장비 제어 시 스마트 제어 접근 허용 절차를 제안하였으며, 통신 데이터 보호 및 사용자 인증 방법으로 다중 암호화 프로토콜을 이용한 데이터 전송 방법과 단말기 고유 정보 및 Q&A를 이용한 사용자 인증 방법 제안하였다. 구현된 스마트 제어 시스템의 성능을 평가하기 위해 스마트 제어 시스템의 동작 실험과 사용자 인증 비교 실험을 하였으며, 장비에 적용 시 장점을 파악하기 위한 실험에서 스마트 제어 시스템은 티칭 팬던트 보다 편리하게 티칭 조작이 가능하였고, 다양한 정보 취득과 하드웨어 조작이 가능하였다. 또한, 스마트 제어 시스템 적용 시 장비의 에러 조치 시간을 약 13% 단축할 수 있었다.

Abstract Smart devices are used in a variety of industries, because applications for them are easy to develop and portable. However, industrial equipment can cause security problems for information and accidents when controlling the actuator of the equipment at a remote location. In this paper, we studied methods of solving these problems and the advantages of applying smart control systems to industrial equipment. We propose a manual manipulation method using queries and a smart control access procedure for controlling equipment using a smart device. In addition, we propose a data transmission method employing multiple encryption protocols and a user authentication method using unique information from the smart device and Q & A as the communication data protection and user authentication methods, respectively. In order to evaluate its performance, an operation test of the smart control system and user authentication comparison experiment were performed. In order to understand the advantages of applying the smart control system to the equipment, we conducted a comparative experiment with a teach pendant and evaluated its reaction time in case of error.

Keywords : FA, Industrial Equipment, Mobile Control, PC Control, Smart Control

1. 서론

오늘날 스마트폰의 보급으로 장소에 상관없이 언제 어디서나 인터넷에 접속이 가능하다. 특히 무선네트워크, 센서 기술의 발달 및 스마트폰과 같은 지능화된 단말기의 보급은 정보의 활용성을 높이며 산업 전반으로 확대되고 있다. 또한, 스마트 기기의 사양 발전과 다양한 디바이스의 내장으로 애플리케이션 개발 시 별도로 디바

본 논문은 2015년도 중소기업청 첫걸음 산학연협력 기술개발 지원 사업에 의해 연구되었음.
*Corresponding Author : Hwang-Rae Kim(Kongju National Univ.)
Tel: +82-41-521-9227 email: plusone@kongju.ac.kr
Received November 11, 2016 Revised (1st March 6, 2017, 2nd April 4, 2017)
Accepted April 7, 2017 Published April 30, 2017

이스들을 구입할 필요가 없어 이에 따른 비용을 절감할 수 있다[1-3].

스마트 기기는 휴대하기 편리하고 애플리케이션 개발이 쉬운 장점으로, 산업 전반에서 많이 이용되고 있다. 그러나 산업용 자동화 장비 시장에서는 장비에서 제공되는 정보에 대한 보안 문제 및 원격지에서 장비의 액추에이터를 제어 시 발생할 수 있는 사고 등으로 국내의 많은 기업에서 스마트 제어 시스템의 적용을 미루고 있다.

위와 같은 문제에 대해 본 논문에서는 아래와 같이 세 가지 문제점을 제시하고, 이를 해결하기 위한 방법으로 사용자 인증 방식, 통신 프로토콜 암호화 방법 및 스마트 제어 접근 허용 절차를 설계하였으며, 스마트 제어 시스템 적용 시 장점에 관한 연구를 수행하였다.

첫째, 장비의 가동 현황, 생산정보, 장비 Maker 등은 기업의 생산 성능의 지표로 활용되므로 승인되지 않은 사용자에게 정보를 유출해서는 안 된다.

둘째, 다른 장비 사용자가 장비를 조작 중에 원격지에서 모터 및 솔레노이드와 같은 액추에이터를 제어하면 사고가 발생할 수 있다.

셋째, 터치스크린이 잘못 눌려 오동작이 발생할 수 있다.

2. 스마트 제어 시스템 적용 분야

2.1 산업별 적용 분야

최근 IOT에 관한 연구 개발이 활발히 이루어짐에 따라 스마트 기기를 이용하는 분야로 제조, 헬스, 에너지, 홈, 자동차, 교통 등의 다양한 분야에서 이용하고 있다[4]. 예를 들어, 스마트 기기를 이용하여 자신의 운동량을 점검할 수 있고, 가정 내의 보일러 및 조명 등을 원격지에서 제어가 가능하며, 원격지에서 공장의 CCTV를 감시하는 등 다양하게 이용되고 있다.

Fig. 1. Smart Control Screen

현재 산업에서 스마트 기기를 이용하는 대부분의 제어 시스템에서는 단순 기능에 대한 ON/OFF 동작을 수행하거나 일반적인 정보를 취득하는 행위가 대부분이다. 그러나 산업용 장비에서는 액추에이터 구동에 따른 안전 문제 및 관련 정보의 보안 문제 등으로 이를 고려하여 스마트 제어 시스템 구현하여야 한다.

Fig. 1은 구현된 스마트 제어 시스템으로 산업용 장비의 동작을 제어하는 화면을 나타낸다.

2.2 티칭 조작 장치

티칭 조작이란, 로봇 또는 모터의 기준 위치를 정하는 행위를 말하는 것으로, 대부분의 산업용 장비는 별도의 운영 화면에서 티칭 조작을 수행한다. 그러나 공정 장비와 같이 장비 크기가 큰 장비에서는 운영 화면과 티칭 조작하고자 하는 대상체가 멀리 떨어져 있어, 운영 화면에서 직접 티칭 조작하기 어려우므로, 티칭 펜던트(이하 TP) 등을 이용하여 티칭 조작을 수행하고 있다.

기존에 사용하고 있는 TP는 유선으로 연결되고 텍스트 기반의 프로그래밍 사용 및 버튼 조작을 통해 티칭 작업을 수행하기 때문에 어려움이 있다. 그러나 본 논문에서 제시하는 스마트 제어 시스템에서는 산업용 장비의 정보 취득 및 하드웨어 조작 등의 제어 기능을 가지고 있어, 현재 제조 현장에서 많이 사용되고 있는 TP의 기능을 대신할 수 있으며, 스마트 기기의 장점인 그래픽 환경과 터치 기능을 적용하여 손쉽게 티칭 조작을 할 수 있다. 또한, 무선으로 연결되기 때문에 더욱 편리하게 티칭 조작이 가능하다. Fig. 2는 티칭 조작을 위해 기존에 사용하고 있는 티칭 조작 장치를 나타낸다[5][6].

(a)Teaching pendent (b)Joystick (c)Universal joint

Fig. 2. Teaching Unit of Industrial Equipment

3. 스마트 제어 시스템 설계

3.1 시스템 구성

본 논문에서 설계한 스마트 제어 시스템에서는 스마트 기기를 이용하여 내부 또는 외부에서 스마트 제어 서버에 접속을 통해 장비의 다양한 정보 취득 및 원격지에서 장비를 제어하는 서비스를 제공한다. 이런 스마트 제어 시스템을 구성하기 위해서는 Fig. 3에서 보는 바와 같이 스마트 기기, 네트워크, 스마트 제어 서버 및 산업용 자동화 장비로 구성할 수 있다.

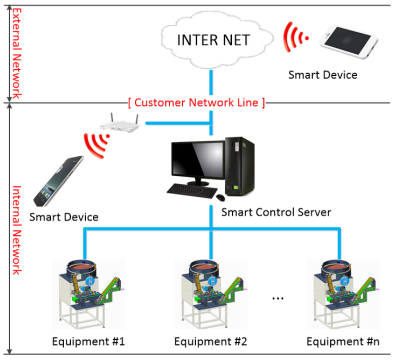

Fig. 3. Smart Control System Diagram

3.2 사용자 등록 절차

일반적으로 사용자가 스마트 기기를 이용하여 서비스를 받고자 하는 경우, 온라인 사이트를 이용하여 관련 업체 사이트의 회원에 가입하고 서비스를 받고 있다. 이는 대다수를 대상으로 서비스를 제공하기 때문이다. 그러나 본 논문에서 제시하는 스마트 제어 시스템의 사용자 등록 방법은 장비의 사용자가 등록 권한을 가진 관리자에게 서비스 이용을 요청하면, 해당 관리자가 사용자의 적합성을 판단하여 사용자 등급 및 고유 정보를 취득한 후 서버에 등록하는 방식으로 사용자 등록을 진행한다. 이는 장비 특성상 장비를 운영하고 관리하는 한정된 소수자에게만 권한이 부여되기 때문이다.

Fig. 4는 스마트 제어 시스템의 사용자 등록 과정을 나타내는 것으로, 사용을 원하는 사용자가 관리자에게 사용 등록을 요청하면 관리자는 사용자의 적합성을 판단하여 서비스 허가 여부를 결정한다. 서비스가 허용된 사용자에 대해 관리자가 사용자 등급을 결정하고, 이후 사용자 인증 수단으로 사용할 사용자의 단말기 고유 정보인 Mac 주소, 전화번호 등의 물리적인 정보를 취득하고, 사용자 접속 시 사용되는 사용자 ID와 Password 및 매뉴얼 조작 시 질의에 사용되는 정보에 대해 사용자가 직접 질의 및 응답(Q&A)에 대한 5개 이상의 정보를 입력하여 스마트 제어 서버에 등록하게 된다. 이후, 등록된 사용자는 등록된 단말기와 사용자가 입력한 고유 정보를 이용하여 서버 시스템에 접속한 후 사용자 등급에 따른 서비스를 받을 수 있다.

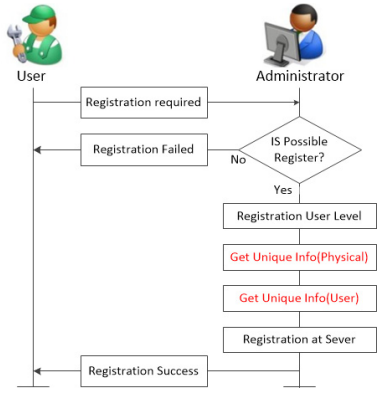

Fig. 4. User Registration Process

3.3 사용자 인증 설계

스마트 제어 시스템의 서비스를 받기 위해서는 승인된 사용자에게만 서비스가 제공되어야 하므로 사용자 인증 절차를 걸치게 된다. 사용자 인증 방식에는 크게 지식기반, 소유 기반, 생체 기반 인증기술로 나눌 수 있으며, 인증 시 보안 강도가 높으면 사용자 접근이 어렵고, 관련 투자비용이 많이 발생하는 단점이 있다[7][8].

이런 이유로 대다수 서비스를 제공하는 업체에서는 서비스 제공 범위에 따라 보안 강도를 조절하여 사용하고 있다. 상대적으로 보안 강화가 필요한 국내 은행을 예를 들면, 서비스 접속 시 사용자 ID 또는 패스워드와 같은 지식기반 인증을 수행하고, 금액 이체 시 OTP, 보안카드와 같은 소유기반 인증을 수행하고 있다. 생체 기반 인증은 보안 강도는 높으나, 생체기반 인증을 수행하기 위해서는 지문 인식과 같은 서비스가 제공되는 단말기를 구입해야하는 불편함이 있다.

이런 이유로 본 논문에서는 로그인 시 지식기반 인증을 수행하고, 소유 기반의 인증의 하나로 사용자 등록 시 미리 등록된 단말기의 고유정보인 Mac 주소와 전화번호를 이용하여 로그인을 수행하도록 설계하였다. 또한, 단말기 분실 등의 문제가 발생할 수 있으므로, 사용자 등록 과정에서 등록한 Q&A 정보를 이용하여 재차 승인된 사용자임을 확인하여 보안 강도를 높였다. 일반적으로 Q&A 정보는 ID 또는 Password 분실 시 분실한 사용자

임을 확인하기 위해 미리 업체에서 제시된 질의에 대한 답(일반적으로 1개 등록)을 하도록 하여 인증을 수행하고 있으나, 본 논문에서 제시한 Q&A는 사용자가 직접 질의하고 답하도록 하는 방식과 5개 이상의 질의 데이터를 등록하여 이를 임의로 산출하여 질의하는 방식으로 설계하였다.

$$P = \frac{k}{n} \quad (1)$$

식 (1)은 Q&A 질의 방식에서 암호 해독의 경우의 수를 나타내는 것으로, P는 암호 해독 확률, n은 질의의 개수, k는 비밀 정보 유출로 승인되지 않은 사용자가 알고 있는 암호의 개수를 의미한다. 기존 Q&A 방식에서는 n=1이므로 k=1인 경우 암호 해독이 가능하다. 그러나 본 논문에서 제시한 방법에서 n>=5이므로 n=5로 가정하면, k=5가 되어야 모든 암호 해독이 가능하므로 이전 Q&A 방식보다 보안 강도가 높음을 알 수 있다.

Fig. 5는 사용자가 서비스를 받기위해 사용자 인증을 걸쳐 Login을 수행하는 과정을 나타낸다.

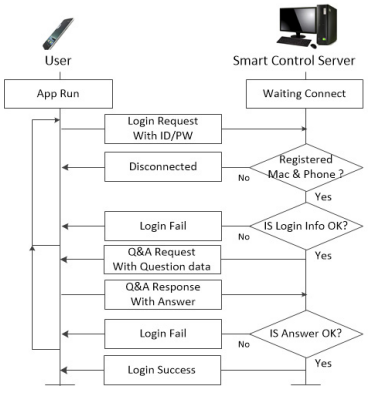

Fig. 5. Login Procedure

3.4 서비스 제공 범위 설계

산업용 장비를 관리하고 운영하는 측면에서 조작 권한이 없는 사용자가 장비의 모터 또는 I/O와 같은 하드웨어 조작을 수행하거나 스마트 기기를 이용하여 원격지에서 장비를 제어하면 사고가 발생할 수 있다. 이런 이유로 대부분의 장비 업체에서는 운영자, 정비사, 관리사와 같이 사용자에 등급을 부여하여 장비의 조작 범위를 제한하고 있으며, 제조 현장에서 장비 운영은 사용자가 직접 장비 앞에 있을 때만 운영이 허용되고 있다. 이런 이유로, 스마트 제어 시스템에서는 사용자 등급 및 접속 위치에 따라 서비스 제공 범위의 정의가 필요하다.

Table 1은 본 논문의 스마트 제어 시스템에서 제안하는 서비스 제공 리스트를 나타내는 것으로, 크게 세 가지로 나눌 수 있다.

첫째, 정보 제공 항목으로 장비 가동현황, 생산 정보, 설정 및 에러 정보 등이 있다.

둘째, 제어 항목에서는 장비를 동작 또는 정지시키거나 Motor 및 I/O와 같은 하드웨어 조작 및 티칭 조작 등을 수행한다.

셋째, 호출 항목은 담당자를 호출하는 기능으로, 장비의 문제 발생 등으로 특정 담당자를 호출할 시 사용하는 기능이다.

Table 1. Information List of Smart Control System

List	Description
Information List	- Product / Run rate info. - Setting and Error Info
Control List	- Equipment Run/Stop control - Motor and I/O control - Teaching operation
Call Function	- call the person in charge

정보 제공 항목은 장비의 생산 능력 등을 판단할 수 있어 정보의 외부 유출에 대한 보안이 필요한 항목이며, 제어 항목은 장비를 직접 구동할 수 있으므로 장비 앞에서만 조작이 이루어져야 한다. 이런 이유로 본 논문에서는 사용자 등급별 권한 및 접속에 위치에 따라 Table 2와 같이 정보 제공 범위를 설계하였다.

Table 2. User Level Permissions

List \ Level		Operator	Maint	Admin
Internal	Call Function	○	○	○
	Information	○	○	○
	Control	×	○	○
External	Call Function	○	○	○
	Information	×	×	○
	Control	×	×	×

3.5 다중 암호화 프로토콜 설계

다중화 암호화 프로토콜은 전송되는 메시지를 해킹으로부터 보호하기 위해 설계된 프로토콜로, 스마트 기기와 서버 시스템 간의 메시지 전송 시 수시로 변경할 수 있는 암호키를 이용한 암호화 알고리즘 적용하여 같은 데이터 메시지에 대해 서로 다르게 전송함으로써 외부

침입으로부터 메시지의 해독을 더욱 어렵게 하기 위해 설계되었다. 다중 암호화 프로토콜은 Fig. 6에서 보는 바와 같이 암호화 알고리즘의 종류를 선택하는 Encrypted Index와 Security Key를 선택하는 암호키 영역과 실제 데이터 메시지를 포함하는 메시지 영역으로 구성되어 있다.

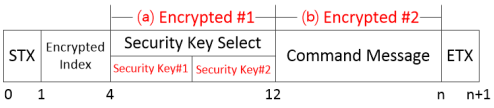

Fig. 6. Multiple Encryption Protocol Format

Fig. 7은 암호키를 선택하는 과정을 나타내는 것으로 단말기가 처음 서버에 접속되면 단말기와 서버 간에 키 값이 다를 수 있으므로 초기 접속 후 단말기가 가지고 있는 암호키 값을 서버에 전송한다. 이 경우 서로의 암호키를 모르기 때문에 Fig. 6의 암호화 Index에서 암호키를 모르더라도 서로 정해진 규칙에 의해 암호 및 해독을 할 수 있는 암호화 알고리즘을 선택하여 암호키를 전송한다. 서버에서 단말기의 암호키를 수신하면 다음에 사용할 새로운 암호키를 단말기에 전송하여 앞으로 메시지 송수신 시 사용할 암호키를 공유하게 된다. 이후 암호화 Index에 암호키를 이용한 암호화 알고리즘을 선택하고 공유된 암호키를 이용하여 데이터 송수신 시 사용하게 된다. 또한, 서버에서 설정된 특정 조건에 의해 새로운 암호키를 계속 발급함으로써 외부의 침입자에 의한 해독을 더욱 어렵게 하였다.

다중 암호화 알고리즘 사용하면 사용된 암호화 알고리즘 형태에 따라 해독의 경우의 수가 더욱 복잡하게 된다. 예를 들어, 일반적으로 하나의 암호키를 사용하는 암호화 알고리즘의 메시지 해독의 경우의 수를 2^n이라고 가정할 경우, 제안하는 다중 암호화 프로토콜에서는 2^n의 메시지 영역의 암호 해독의 경우의 수와 암호키 선택 영역의 암호의 해독의 경우의 수를 2^k라 가정하면, $2^n * 2^k = 2^{n+k}$의 해독의 경우의 수가 나타나 일반적인 프로토콜에서 메시지 영역만 암호화하는 것에 비해 2^k만큼 해독이 어렵게 된다. 또한, 암호화 Index를 변경하여 여러 개의 암호화 알고리즘을 적용한다면 해독의 경우 수는 더욱 복잡해지므로 외부 침입으로부터 해독은 더욱 어렵게 된다.

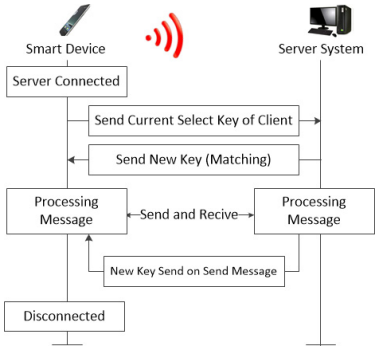

Fig. 7. Security Key Select Process

3.6 스마트 제어 접근 허용 절차 설계

스마트 제어 시스템에서 제공되는 하드웨어 원격 제어 기능을 다른 사용자가 장비 점검 중에 멀리 떨어진 위치에서 사용할 경우 사고가 발생할 수 있다. 이런 문제로 스마트 제어 시스템을 이용한 하드웨어 원격 제어 시에는 항상 장비의 상태를 확인할 수 있는 위치에서만 조작되어야 한다. 이를 해결하기 위해 본 논문에서는 스마트 제어 접근 허용 절차를 설계하였다.

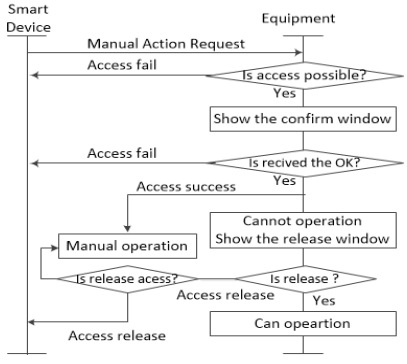

Fig. 8. Smart Control Access Procedure

Fig. 8은 스마트 제어 접근 허용 절차를 나타내는 것으로 스마트 기기에서 서버 시스템에 H/W 조작을 위한 스마트 제어 허용 요청을 수행하면 서버에서는 접근 권한 검사 및 “화면에 스마트 제어 동작을 진행하시겠습니까?”의 메시지를 출력하여, 사용자가 특정 시간 안에 “예” 응답을 선택하면 접근이 허용 된다. 접근이 허용되면 장비의 조작은 스마트 기기에서만 가능하며, 스마트 제어가 완료될 때까지 장비는 가동할 수 없다. 스마트 기기에서 모든 작업을 완료하면 스마트 제어 허용을 해제한 후, 장비를 정상 가동할 수 있다. 또한, 스마트 기기 제어 시 특정 시간 동안 사용자가 동작을 수행하지 않는

경우 서버에서 스마트 기기에 사용자 등록 시 등록한 고유 정보를 이용해 Q&A 인증을 수행하며 잘못된 응답 시 강제 해제를 수행할 수 있다.

또한, 스마트 기기는 터치스크린을 이용하여 동작하므로 스마트 제어 접근이 허용된 상태에서 터치스크린이 잘못 눌려 오동작이 발생할 수 있다. 이런 오동작으로 인해 다른 사용자가 장비 내에서 작업 중에 장비의 모터 등을 움직이게 되면 사고가 발생할 수 있으므로, 모터와 같은 액추에이터 동작 명령에서는 항시 작업자에게 특정 값을 입력하도록 질의를 수행하여 그 값이 특정 시간 안에 입력되었을 경우에만 동작할 수 있도록 설계하였다.

4. 실험 결과

본 논문에서 제시한 스마트 제어 시스템의 실험을 위해 병원에서 피 검사 시 사용되는 진공 채혈관의 조립 공정에서 진공 채혈관 튜브를 공급하는 장비에 적용하여 실험을 수행하였다.

4.1 스마트 제어 시스템 동작 실험

본 실험은 스마트 제어 시스템의 정상적인 동작 여부를 판단하는 실험으로 정부 기관 산하 인증기관인 K 인증기관으로부터 실험을 수행하였다. Fig. 9는 스마트 제어 시스템의 실험 화면을 나타내며, 실험 방법으로는 스마트 기기를 서버시스템에 접속 절차에 따라 접속한 후, 25회 장비 조작 관련 제어 지령을 내려 동작 상태를 확인한 결과, Table 3과 같이 25회 모두 정상 동작하는 것을 확인하였다. 또한, 정보 취득에 관한 자체 평가에서는 Fig. 9에서 보는 바와 같이 장비의 정보가 스마트 기기에 정상적으로 전달되는 것을 확인하였다.

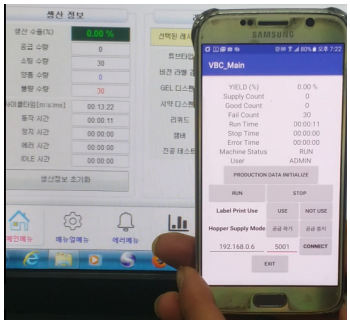

Fig. 9. Smart Control Test Screen

Table 3. Test Resut of Smart Control Operation

No	List	Count
1	Operation Success	25
2	Operation Error	0

4.2 사용자 인증 비교 실험

본 논문에서 제시한 인증 설계에 대한 실험을 수행하기 위해 국내 금융기관인 H 은행의 인증 방식과 비교하였다.

Table 4에서 보는 바와 같이 Login 단계인 1단계에서는 국내 H 은행과 동일한 ID/Password 방식의 지식 인증 기반을 사용하였으며, 2단계의 소유기반 인증에서는 보안카드, OTP 인증을 대신하여 단말기 고유 정보를 이용하였다. 또한, 3단계에서는 공인 인증서를 대신하여 정보의 확장이 가능한 Q&A 인증을 수행하도록 설계하였다. 마지막으로 데이터 보안 단계에서는 H 은행에서 사용하는 별도 보안 모듈을 대신하여 다중 암호화 프로토콜을 설계하였다.

Table 4. User Authentication Comparison

Step	H Bank	This Paper
Step 1	ID/Password	ID/Password
Step 2	Security Card or OTP	Smart device physical Info
Step 3	Certificate Authority	Multiple Q&A
Data Security	Use Security Module	Use Multiple Encryption Protocol

Table 5는 인증 수단 관련 자체 평가를 한 결과로 1단계인 로그인 시 사용되는 지식 기반 인증의 ID/Password 방식에서는 동일한 결과를, 소유 기반 인증인 2단계에서는 보안 카드는 복사할 수 있고, OTP의 경우 별도의 번호를 발생하여 이를 확인하여야 한다는 점에서 단말기의 물리적인 정보를 사용하는 본 논문이 보안성과 편리성에서 더 우수하다고 판단하였으며, 3단계에서는 공인인증서가 Q&A보다 보안 강도는 높게 판단하였으나, 기업 내에 서버를 이용한다는 점과 편리성 면에서 Q&A 방식의 인증 방식도 만족한 결과를 얻었다고 판단하였다. 그러나 데이터 보안 항목에서는 보안 기법이 서로 다르고, 보안 모듈의 암호화 방법이 공개되지 않는 점으로 비교 대상에서는 제외하였다.

Table 5. Comparative results

H Bank	This Paper	Result
ID/Password	ID/Password	Same
Security Card or OTP	Smart device physical Info	Good
Certificate Authority	Multiple Q&A	Satisfaction

4.3 티칭 펜던트와의 비교 실험

현재 공정 장비 등에서 많이 사용하고 있는 티칭 펜던트(TP)는 티칭 조작에 한정된 서비스를 제공하고, 유선 장치에서 텍스트 및 버튼 기반으로 티칭 조작을 수행한다. 그러나 스마트 제어 시스템에서는 생산, 에러 정보 등과 같은 다양한 정보 제공이 가능하고, 티칭 조작뿐만 아니라 장비의 다른 H/W 조작이 가능하며, 사용자 등급 설정 등으로 서비스 범위를 제한할 수 있다. Table 6은 티칭 펜던트(TP)와 스마트 제어 시스템과의 비교 결과를 나타낸다.

Table 6. Smart Control & Teaching Pendent Comparison

List	Teaching pendent	Smart control
User level	Impossible	Possible
H/W operation	Limited (Teaching only)	All H/W operation
Teaching	Possible	Possible
Service	Limited (Teaching only)	The various services (product, error)
Operation	- text-based - Button operation	- Graphic-based - Touch operation
Connect	wire connection	wireless
Device	Dedicated devices	Smart devices

4.4 에러 조치 시간 실험

본 실험은 산업용 자동화 장비인 진공 채혈관 튜브 공급 장비에 스마트 제어 시스템을 적용하여 에러 발생 시 조치 시간에 관한 실험으로, 공급 버퍼 부에 자재가 걸린 에러에 대한 조치 시간을 측정하여 실험하였다. 실험 시 사람에 의한 오류를 최소화하기 위해 실험 대상자는 경력 19년의 장비 개발 경험을 가지고 있고, 해당 장비를 직접 개발한 개발자를 대상으로 하였다. 또한, 에러 인식 및 조치 능력에 대한 오류를 최소화하기 위해 2개월 동안 장비를 가동하면서 직접 에러를 조치하여 얻은 학습 효과로 에러 발생 시 바로 조치가 가능한 시점에 실험을 수행하였다.

Fig. 10은 튜브 공급 장비의 에러 발생 위치를 나타내는 것으로, ①은 공급 버퍼부, ②는 튜브 회전부, ③은 에러 발생 위치, ④는 튜브가 버퍼에 걸린 형태를 나타낸다. 실험의 공평성을 위해 동일한 실험자에게 동일한 에러 발생 시 스마트 제어 시스템의 적용 여부에 따른 조치 시간을 총 10회에 걸쳐 측정하였다. Table 7은 실험 결과를 나타내며, 스마트 제어 시스템을 적용 시 약 19.8초의 조치 시간이 빠르게 나타나 약 13%의 에러 조치 시간을 단축하였다.

에러가 발생하면 작업자는 에러 확인, 에러 조치, 장비 가동의 단계를 거친다. 그러나 가동 후 에러가 해결되지 않은 상태에서는 다시 에러가 발생하여 위 과정을 반복하게 된다. 그러므로 에러 조치 완료 시간 T는 식(2)에서 보는 바와 같이 에러 확인시간(E_i), 에러 조치시간(E_p), 장비 가동시간(E_r)과 에러 발생 반복 횟수(n)을 곱한 시간을 말한다. 위 결과는 운영화면과 멀리 떨어진 튜브 공급 장비에서 스마트 제어 시스템을 이용하면 장비 가동 시간(E_r)이 1초 이내에 처리되기 때문에 적용 이전보다 해당 시간(E_r)을 단축 시켜 약 19.8초의 시간 단축이 가능하였다.

$$T=(E_i+E_p+E_r)*n \tag{2}$$

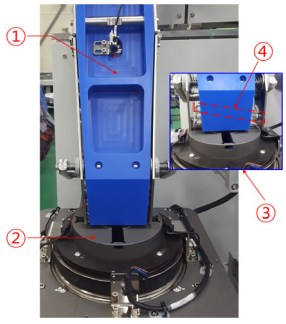

Fig. 10. Error Position Image

Table 7. Apply Result of Smart control system

no.	Apply before (sec)	Apply after (sec)
1	152	131
2	181	143
3	127	105
4	213	154
5	176	135
6	143	163
7	148	100
8	136	158
9	153	142
10	116	116
AVG	154.5 sec	134.7 sec

5. 결론

본 논문에서는 스마트 제어 시스템을 산업용 장비에 적용할 시 발생할 수 있는 문제 해결 방법으로 승인된 사용자에게만 서비스를 제공하기 위한 사용자 인증 설계 및 다중 암호화 프로토콜을 설계하였고, 원격지에서 스마트 제어 수행 및 터치스크린이 잘못 눌려 발생할 수 있는 사고를 막기 위해 스마트 제어 접근 허용 절차와 질의에 의한 하드웨어 조작 방법을 설계하였으며, 스마트 제어 시스템의 실험을 위해 진공 채혈관 튜브 공급 장비에 적용하여 실험을 수행하였다. 국내 K 인증기관에 의뢰하여 수행한 동작 실험에서는 25회 제어 지령을 내려 25회 모두 제어가 정상으로 동작하는 것을 확인하였으며, 사용자 인증 항목에서는 국내 H 은행의 인증 방법과 본 논문에서 설계한 인증 방식을 비교한 자체 평가에서 모두 만족한 결과를 나타내었다. 또한, 스마트 제어 시스템을 산업용 장비에 적용 시 장점을 파악하기 위해 티칭 펜던트와의 비교 실험 및 에러 발생 시 조치 시간에 관한 실험을 수행한 결과, 티칭 펜던트는 한정된 티칭 조작만이 가능하지만, 스마트 제어 시스템에서는 다양한 정보 취득 및 티칭 조작뿐만 아니라 다양한 하드웨어 장치 조작과 권한 설정이 가능하였고, 스마트 제어 시스템 적용한 결과, 에러 발생 시 조치 시간을 약 13% 단축하였다.

향후 연구에서는 스마트 제어 시스템에서 산업용 장비의 다양한 정보를 취득하고, 이를 이용하여 장비의 성능을 향상 시킬 수 있는 방법에 관한 연구를 수행하고자 한다.

References

[1] Soo Jeong, Jong Jin Lee, Won Ki Jung, "A Indoor Management System using Raspberry Pi", Journal of the Korea Academia-Industrial cooperation Society, vol. 17, no. 9, pp. 745-752, 2016.
DOI: http://dx.doi.org/10.5762/KAIS.2016.17.9.745

[2] Min J Kim, Seol B Bae, Moon G Joo, Won Change Lee, "Development of Android Smart phone Application for Mobile Robot Control", Journal of KIIT, vol. 12, no. 5, pp. 7-13, 2014.

[3] Chae-Young Moon, Kwang-Ki Ryoo, "Development of Intelligent Service Robot using Smart Phone based on Android OS", Journal of the Korea Academia-Industrial cooperation Society, vol. 13, no. 9, pp. 4193-4199, 2012.
DOI: http://dx.doi.org/10.5762/KAIS.2012.13.9.4193

[4] Yeong-Jin Kim, Dong-Hwan Kim, "Application and Applied cases of IOT", Journal of the KSME, vol. 56, no. 3, pp. 37-41, 2016.

[5] Sanghun Pyo, Syed Hassan, Yasir Jan, Jungwon Yoon, "Design of 6-DOF Manipulator Intuitive Teaching System Using Smart Phone Orientation: User Friendly and Intuitive Teaching Operation for 6-DOF Manipulator", IEEE 2013 4th International Conference on Intelligent Systems, Modelling and Simulation, pp. 363-369, 2013.
DOI: https://doi.org/10.1109/ISMS.2013.115

[6] Eun Ji Park, Seo Kyeong Eun, Tae Gon Park, Sun Duk Han, Hyeon joong Cho, "A Visual Programming Environment on Tablet PCs to Control Industrial Robots", Journal of KIPS, vol. 5, no. 2, pp. 107-116, 2016.
DOI: http://dx.doi.org/10.3745/KTSDE.2016.5.2.107

[7] Y-J Choi, "ID/PW-based Enhanced User Authentication System design and implementation using a Smartphone", Master's Thesis, PaiChai University, 2015.

[8] A. Hiltgen, T. Kramp, T. Weigold, "Secure Internet banking authentication", IEEE Security & Privacy, vol. 4, no. 2, pp. 21-29, 2006.
DOI: https://doi.org/10.1109/MSP.2006.50

김 보 헌(Bo-Heon Kim) [정회원]

- 2004년 2월 : 호서대학교 컴퓨터공학과 공학사
- 2013년 8월 : 공주대학교 IT공학과 공학석사
- 2016년 8월 : 공주대학교 컴퓨터공학과 박사수료
- 2015년 3월 ~ 현재 : ㈜이지에스 기술이사

<관심분야>
장비 제어 프로그램, 스마트 제어, 스마트 팩토리, IOT 컴퓨터 네트워크, 네트워크 보안, 개발 표준화

김 황 래(Hwang-Rae Kim) [정회원]

- 1982년 8월 : 중앙대학교 전자계산학과 이학사
- 1991년 2월 : 중앙대학교 대학원 컴퓨터공학과 공학석사
- 2007년 8월 : 대전대학교 대학원 컴퓨터공학과 공학박사
- 1983년 3월 ~ 1994년 2월 : 한국전자통신연구원 책임연구원
- 1994년 3월 ~ 현재 : 공주대학교 컴퓨터공학부 교수

<관심분야>
컴퓨터 네트워크, 네트워크 보안, 네트워크 생존성관리, 스마트 제어