https://doi.org/10.33778/kcsa.2024.24.1.043

이중 MCU를 활용한 IoT 보안 교육용 하드웨어(해커보드) 설계★

김 동 원*

요 약

교육(education)과 기술(technology)의 융합이 강조되면서 에듀테크가 교육 현장에 적용되어 다양한 매체와 학습 상황 속에서 학습자 중심의 맞춤형 교육환경을 제공하고 있다. 본 논문에서는 사이버보안 교육 현장에서 사물인터넷 보안 교육을 위한 에듀테크 기반의 교육용 교구를 제작하기 위하여 하나의 보드(Board) 내에서 이중 MCU를 기반으로 공격과 방어가 각각 수행될 수 있도록 하드웨어를 설계하였으며, 사물인터넷의 다양한 센서를 활용하기 위하여 모듈형으로 설계하여 제시하였다. 교육 측면에서 에듀테크를 활용한 사이버보안 교육은 실제 물리적인 교구를 활용함으로써 교육에 대한 호감을 키우고, 임베디드 하드웨어와 소프트웨어, 센서 네트워크 등 기존 교육에서 다루기 어려운 분야에 대한 보안 교육 환경을 간단하게 구성하기 위하여 IoT 보안 교육용 하드웨어 설계시 참고가 될 수 있도록 연구 제안한다.

Design of Hardware(Hacker Board) for IoT Security Education Utilizing Dual MCUs

Dong-Won Kim*

ABSTRACT

The convergence of education and technology has been emphasized, leading to the application of educational technology (EdTech) in the field of education. EdTech provides learner-centered, customized learning environments through various media and learning situations. In this paper, we designed hardware for EdTech-based educational tools for IoT security education in the field of cybersecurity education. The hardware is based on a dual microcontroller unit (MCU) within a single board, allowing for both attack and defense to be performed. To leverage various sensors in the Internet of Things (IoT), the hardware is modularly designed. From an educational perspective, utilizing EdTech in cybersecurity education enhances engagement by incorporating tangible physical teaching aids. The proposed research suggests that the design of IoT security education hardware can serve as a reference for simplifying the creation of a security education environment for embedded hardware, software, sensor networks, and other areas that are challenging to address in traditional education..

Key words : educational IoT security, hacker board, hardware design

접수일(2024년 02월 06일), 수정일(1차: 2024년 02월 24일), 게재확정일(2024년 03월 04일)

★ 이 논문은 2023년도 건양대학교 학술연구비 지원에 의하여 이루어진 것임.

* 건양대학교/스마트보안학과

1. 서 론

현재 인공지능(AI)이 인간의 삶 속으로 빠르게 파고들고 있다. 2022년 챗GPT 등장과 함께 모든 영역에 AI가 활용되면서 혁신으로 이어지고 있다. 디지털 전환(Digital Transformation, DX)을 넘어 AI 전환(AI Transformation, AX) 시대로 나아가고 있는 것이다. 지능정보사회(intelligence information society)에서는 사물들이 가상 세계를 벗어나 물리적인 현실 세계로 확장되고 연결되어 초연결사회로 나아가고 있다. 초연결사회는 일방향에서 쌍방향을 선택한 정보통신기술의 요체가 되고 있다[1]. WEF(World Economic Forum)에서 'What is hyper connectivity?'라는 주제로 세계경제포럼이 개최되면서 초연결사회가 논의되기 시작하였다[2]. 초연결사회는 사람과 사람, 사람과 사물, 사물과 사물간 연결을 통해 사회 전 분야에 변화와 혁신을 이끄는 사회이며, 사물인터넷(IoT) 기술을 기반으로 하여 진화하고 있는 미래사회를 의미한다[3]. 초연결사회는 상호연결성 등이 증가함에 따라 발생하는 사이버보안 위협은 실제 인명피해가 초래되는 등 그 영향 범위가 커지고 있다[4]. 사이버보안의 패러다임이 확장되고, 사이버 위협으로 발생하는 피해 범위는 실생활에 큰 영향을 미치고 있다. 이러한 상황에 대응하기 위해서는 현재의 전통적인 정보보안 교육 방법에는 한계가 있으며, 초연결사회에서 요구되는 기술과 사물, 사물 간 연결에 따른 보다 종합적인 보안교육이 필요하게 되었다.

교육(education)과 기술(technology)의 융합이 강조되면서 '에듀테크'라는 용어가 주목을 받고 있다[5]. 에듀테크는 IT 기술을 활용한 교육 서비스로 간단하게 정의될 수 있으며[6], 인공지능, 빅데이터, 블록체인, AR/VR, 로봇, 사물인터넷 기반의 첨단 기술과 같은 에듀테크가 교육 현장에 적용되고 있다. 에듀테크 기반 교육에 대한 탐색은 디지털 전환 및 코로나 팬데믹으로 가속화되었으며, 에듀테크가 상당한 규모로 성장하고 있다[7,8]. 에듀테크는 기존의 이러닝(e-Learning)과 스마트러닝(Smart-Learning)보다 더 다양한 매체와 학습 상황 속에서 학습자 중심의 맞춤형 교육환경을 제공할 수 있기 때문에[9], 4차 산업혁명 시대의 교육 패러다임[10]이라고 인식되고 있다.

데이터 기반 기술(data-driven technology)의 중요성이 강조되면서 교육 분야에서도 AI 기술을 학교 현장에 적극적으로 활용하기 위한 논의가 진행되고 있으며, 디지털 기술의 교육 분야 활용을 위한 논의 및 이를 추진하기 위한 노력은 코로나 사태로 인해 급증한 원격교육의 수요와 맞물리면서 더욱 가속화되고 있다[11]. "EdTechXGlobal"의 보고서에 의하면 교육 시장 중 에듀테크 산업의 규모는 2020년 2,520억 달러에 이를 것으로 전망하고 있으며[12], 중소벤처기업부에 따르면 국내 에듀테크 시장 규모는 2021년 7.3조 원에서 연평균 8.5% 성장해 2026년에는 약 11조 원에 이를 것으로 전망된다[13]. 에듀테크를 활용한 ICT 분야 교육활동에 사용되는 보조적인 도구는 많은 교육에서 활용되고 있으며, 이에 따라 과학키트, 유아, 초등 저학년, 중등, 고등, 대학/일반으로 다양한 제품들이 개발되어 보급되고 있다. 대표적으로는 아두이노, 라즈베리파이, 큐브로이드, 엔트리, 스크래치, 레고 등이 대표적이라 할 수 있겠다.

본 논문에서는 정보보안 교육현장에서 사물인터넷 보안 교육을 위한 에듀테크 기반의 교육용 교구를 제작하기 위하여 하나의 보드(Board) 내에서 공격과 방어 기능을 수행할 수 있도록 이중 MCU 탑재를 채택하였으며, 사물인터넷의 다양한 센서를 활용하기 위하여 모듈형으로 설계하였다. 교육 측면에서 에듀테크를 활용한 사이버보안 교육은 실제 물리적인 교구를 활용함으로써 교육에 대한 호감을 키우고, 임베디드 하드웨어와 임베디드 소프트웨어, 센서 네트워크 등 기존 교육에서 다루기 어려운 분야에 대한 보안 교육 환경을 간단하게 제공하여 하드웨어 기반의 보안교육을 완성하는 것에 목적이 있다. 본 연구를 통해서 소프트웨어 기반의 정보보안 교육에서 하드웨어를 활용하는 사이버보안 교육 실천과 발전을 위한 기초연구가 될 것으로 기대한다.

2. 해커보드 설계 전략

이중 MCU를 활용한 IoT 보안 교육용 하드웨어를 설계하기 위해서는 다음을 고려하여야 한다. MCU는 주변 장치(센서, 디스플레이, 구동기 등)와의 통신을 위해서는 ①주변 장치로 명령어 전달, ②주변 장치 상태 확인(명령어 전달에 따른 동작 상태 확인, ③주변 장치로부터 결과 입력, ④주변 장치로부터 입력된 결과를 바탕으로 신호처리 알고리즘 동작, ⑤주변 장치에 새로운 명령어를 전달하거나 추가 데이터 요청 대기와 같은 동작을 수행하기 위해서는 MCU 내의 알고리즘 처리 능력 및 인터페이스 전송 속도가 고려되어야 한다[14]. 센서의 출력은 대부분 아날로그 출력과 디지털 출력이다. Table 1.과 같이 MCU는 이 센서들의 출력을 입력으로 받아 처리할 수 있어야 한다.

〈Table 1〉 센서와 MCU 간 입출력 인터페이스

인터페이스	특징
아날로그	- 온도, 먼지, 빛, 적외선 센서 등 - 센서로부터 획득한 데이터를 전압 값을 조절하여 MCU에 전달되는 방식 - 전압 값을 MCU는 A/D 변환기를 사용하여 디지털 정보로 변경 - 여러 개의 센서로부터 값을 획득할 경우 Multiplexer를 시분할하여 각각의 센서 데이터를 입력받아서 처리
디지털	- 인체저항 감지, 조도, 모터, 타이머 센서 등 - 디지털 데이터로 MCU에 전달하거나 처리된 데이터는 디스플레이 장치로 전송 - SPI, I2C, UART 통신 인터페이스로 MCU는 master, 센서는 slave로 구동 - MCU는 펄스 형태로 센서에 명령을 전달하거나 센서로부터 데이터를 받으며 펄스 주파수나 주파수의 duty 비를 변경하여 센서와 통신

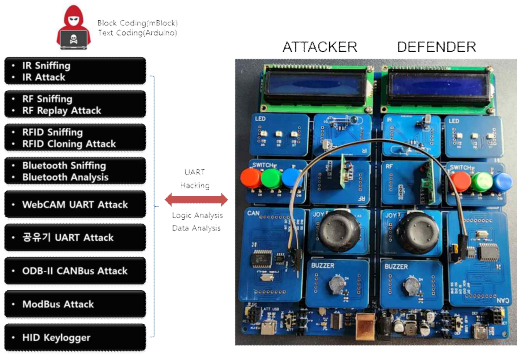
해커보드를 교육에 적용하기 위한 설계를 도출하기 위해서는 모델의 본질적 특성이 순환적 절차의 방법이므로 해커보드 제작을 위한 하드웨어는 반복 사용할 수 있어야 하고, 평가를 통한 업데이트와 개선이 반영되어야 하기 때문에 변형-확장이 용이해야 한다. 또한, 프로그래밍 환경이 편리해야 하며, 하드웨어 기반의 보안 공격과 방어 기능을 제공하여 제한된 교육 환경에서 최대한의 교육 성과를 학생들이 달성하도록 하는 해커보드의 설계전략이 중요하다. 이러한 설계전략을 고려하여 Table 2.와 같이 8가지 설계전략(S1~S8)을 수립하였다.

〈Table 2〉 8가지 설계 전략(S1~S8)

No	설계전략
S1	유지관리 및 보수(쉬운 교체 기능) - 하드웨어 보드 유지-관리 - 재고 관리 및 수리 - 수업 시간 관리
S2	쉽고 빠른 조립-해제 - 정해진 수업 시간안에서 조립과 프로그래밍 - 수업 시간 활용의 효율성 - 개선 및 업데이트의 용이성 확보
S3	센서를 통한 확장의 용이성 - 센서의 개선, 변형 및 발전성 확보 - 커스터마이징, 개선의 용이성 증대
S4	오픈소스(하드웨어, 소프트웨어) - 쉬운 접근과 다양한 변형 - 비용과 시간의 경제성
S5	편리한 프로그래밍 - 대중적 장비를 활용한 프로그래밍 환경
S6	공격과 방어 기능의 편리성 - 목표 대상의 핵심 기능 시뮬레이션 가능 - 공격과 방어의 쉬운 교육 환경 구성
S7	이동의 편리성 - 학교/홈스쿨의 연계성 - 편리한 이동성
S8	가격 경쟁력/낮은가격

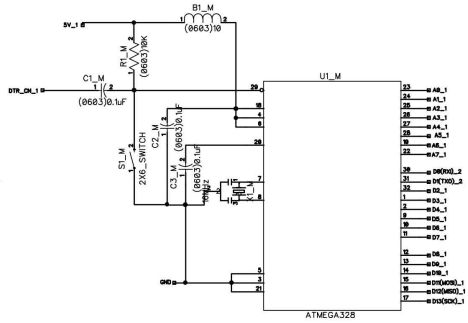
3. 해커보드 하드웨어 설계

본 장에서는 2장에서 제시한 설계전략에 대하여 이를 하드웨어로 구현한 결과를 제시한다. MCU를 직접 설계하기 위해서는 디지털 회로설계, 동작 검증, 온칩 설계에 이르기까지 상당히 많은 전문 과정이 요구된다[15]. Figure 1.은 본 논문에서 설계하고자 하는 해커보드를 제시하였다. 이중 MCU를 탑재하여 대칭하도록 삽입하여 공격과 방어를 하나의 보드에서 구현하도록 설계한다.



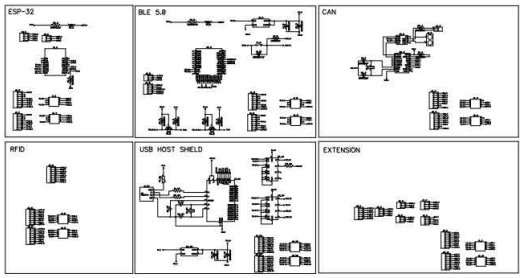
(Figure 1) 해커보드 외형 및 보안교육 기능

설계전략 S1, S2, S3, S4, S5를 달성하기 위한 방법으로 교육용으로 가장 많이 활용되고 있는 MCU(ATmega328P)로 Figure 2.와 같이 설계하였다. ATmaga328P는 오픈하드웨어인 아두이노(Arduino)에서 활용되고 있는 MCU이다.



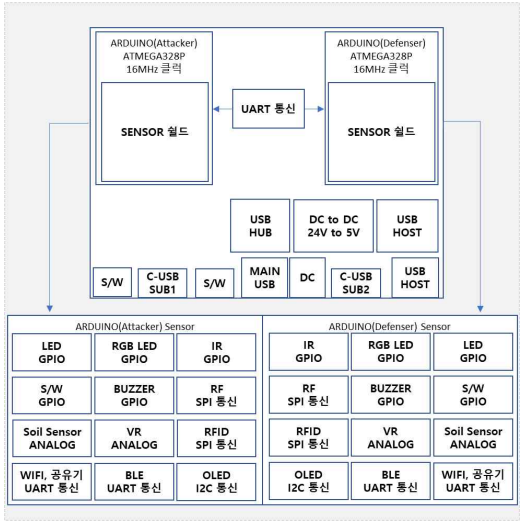
(Figure 2) ATmaga328P MCU로 설계한 회로도

센서는 각각 모듈로 구성하여 Figure 3과 같이 설계하였다.



(Figure 3) ESP-32, BLE, CAN 등 센서 모듈 회로도

MCU와 센서 모듈은 Attacker와 Defenser로 구성하여 이중 MCU를 기반으로 Figure 4와 같이 구성하여 설계하였다.



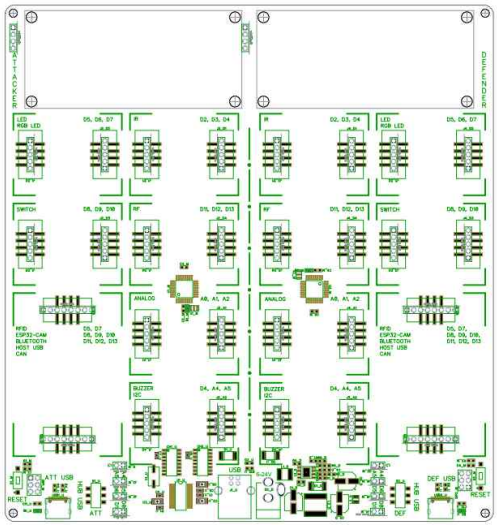
(Figure 4) 해커보드 Functional Diagram

설계전략 S2, S3, S6을 달성하기 위하여 센서들은 모듈화화여 탈부착이 쉽도록 Figure 3.와 같이 설계한다. 또한, 센서 모듈의 탈부착 시 고장이나 접촉 불량과 사용자의 숙련도를 고려하여 해커보드의 기능적 오류를 최소화하기 위하여 센서모듈과 보드는 마그네틱 커넥터 방식으로 설계한다. 다만, 경제성을 고려하여 Table 3.와 같이 3개의 커넥터 타입(핀헤더, 박스헤더, 마그네틱)을 사용자가 선택할 수 있도록 유형을 구분하여 설계한다.

〈Table 3〉 센서모듈 Connect Type

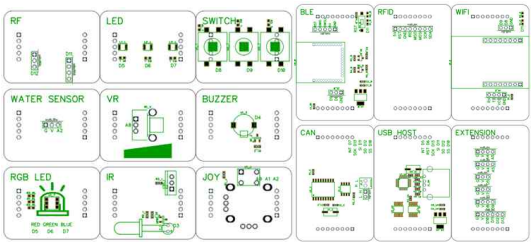
핀헤더	박스헤더	마그네틱
		

메인보드는 이중 MCU를 기반으로 설계하였으며, 센서는 각각 모듈을 기반으로 설계하였으며, 동작 결과를 출력하기 위한 I2C LCD를 기본적으로 장착되도록 Figure 5.와 같이 PCB를 설계하였다.



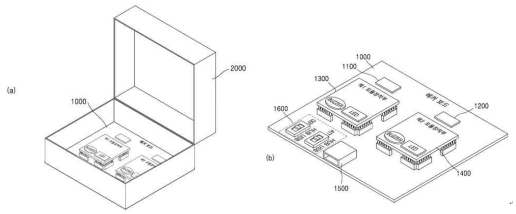
(Figure 5) Main PCB Layout Dimension

센서는 총 15개를 기본으로 구성하고, ESP-32 칩을 활용하여 공유기, 웹캠 구성을 위한 용도로 구성하여 Figure 6.와 같이 Sensor Module PCB Layout Dimension을 설계하였다.



(Figure 6) Sensor Module PCB Layout Dimension

설계전략 S1, S2, S7을 달성하기 위하여 케이스를 포함하고, 해커보드는 모의해킹에 대한 공격 시뮬레이션을 수행하는 1 MCU와 모의해킹에 대한 방어 시뮬레이션을 수행하는 2 MCU, 데이터 입·출력을 담당하는 센서모듈 장착부, 동작여부를 출력하는 출력부(LCD), 컴퓨터장치와 연결하는 인터페이스부, 전원부로 Figure 7.과 같이 설계하였다.



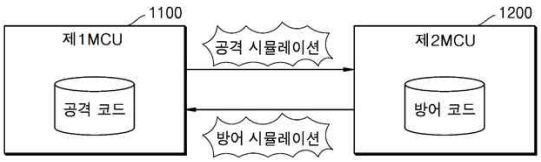
(Figure 7) 해커보드 실습 장치 도면

설계전략 S2, S5, S6을 달성하기 위하여 해커보드는 Table 4.와 같은 기능을 제공하도록 설계하였다. 기본적인 센서들을 학습하는 Basic, Serial 통신을 학습하는 Serial을 기초로 IR, RF, RFID, Bluetooth, UART, OBD-II/CAN, Modbus에 대한 공격과 방어를 기능적으로 동작할 수 있도록 설계하였다.

〈Table 4〉 해커보드 기능 명세

CAT	Function	Description
Basic	Basic Control - 01	LED 점멸 테스트
	Basic Control - 02	RGB LED + 스위치
	Basic Control - 03	피에조부저
	Basic Control 응용	상기 내용 Add 응용하기
Serial	기본 출력	시리얼 모니터 출력하기
	Serial 분석 - 01	Logic analyzer 신호 분석
	Serial 분석 - 02	Baud Rate 및 메시지 분석
IR	IR Sniffer	TV 리모컨 신호 스니핑
	IR Tampering	적외선 신호 분석 후 변조
RF	RF Sniffer	RF신호 스니핑 및 변조
RFID	RFID Cloning	RFID 카드 복제
B/T	Bluetooth Sniffer	B/T 패킷분석 및 스니핑
UART	HID H/W Keylogger	USB 키보드 키로거 제작
	Home Router Hacking	공유기 UART 분석
OT	OBD-II/CAN Hack	CAN 통신 프로토콜 분석
	Modbus Hack	Modbus 프로토콜 분석

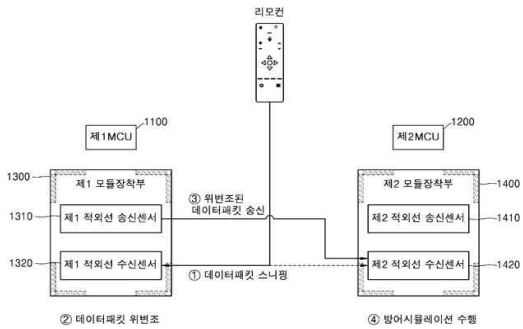
해커보드는 이중 MCU를 탑재하여 공격부(Attacker), 방어부(Defenser)가 독립적으로 동작되고, 프로그래밍을 할 수 있도록 설계하였다. 또한, 방어부는 Table 3.의 기능을 시뮬레이션할 수 있도록 소프트웨어를 함께 제공한다.



(Figure 8) Main Layout Dimension

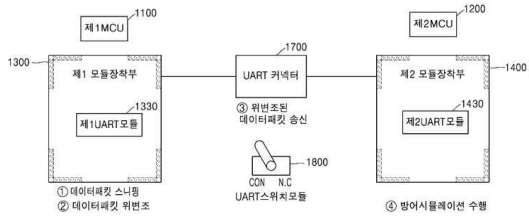
IoT 보안 실습 교육이 어려운 이유는 모의해킹 대상 제품(TV, 자동차, Bluetooth 제품, 드론, RC Car, 디지털도어록 등)을 교육 환경으로 구성하기 어렵다는 것이다. 예로 OBD-II 또는 CAN 통신에 대한 모의해킹 실습 교육을 위하여 환경을 구성하기 위해서는 실제 자동차를 대상으로 하거나 별도의 제품으로 환경을 구성해야 한다. Modbus, IR, RF, RFID 등 모든 실습환경을 각각 구성하는 것은 현실적으로 어렵다. 본 논문에서 제시하는 해커보드는 하나의 보드로 Table 4.의 기능을 시뮬레이션하여 공격과 방어를 위한 프로그래밍과 데이터, 프로토콜 등을 분석할 수 있도록 설계하였다.

예로, 적외선(IR) 통신에 대한 IoT 보안 교육을 위한 실습 시나리오는 Figrue 9.과 같다. 제1 MCU에는 공격용 IR송신, IR수신 센서 모듈과 제2 MCU에는 방어용 IR송신, IR수신 센서 모듈을 각각 장착한다. 방어부(Defenser)에는 제공되는 IR 해킹 프로그램을 업로드하면, IR 통신에 대한 보안교육 환경 구성이 완료된다. 이후 IR Sniffer를 공격부(Attacker)에 프로그래밍하여 방어부가 동작되는 원리와 데이터를 수집/분석하고, 분석한 데이터를 기반으로 IR Attack 프로그램을 작성하여 방어부를 조작할 수 있도록 설계하였다.



(Figure 9) Main Layout Dimension

UART 통신에 대한 보안 교육을 위한 실습 시나리오는 Figrue 10.과 같다. 제1 MCU에는 공격용 UART 모듈과 제2 MCU에는 방어용 UART 모듈을 각각 장착한다. 방어부(Defenser)에는 제공되는 UART 해킹 프로그램을 업로드하여 실행한 후, 메인보드의 UART 스위치 모듈을 선택하여 UART 통신 모드로 변경한다. 이후 Logic Analyzer를 활용하여 공격부에 연결하여 UART 신호를 분석하여 활용할 수 있도록 설계하였다.



(Figure 10) Main Layout Dimension

앞에서 설명한 전략과 방법을 통하여 Figure 1.에 제시된 바와 같이 이중 MCU를 활용하여 공격부와 방어부가 각각 동작되도록 설계함으로써 하나의 보드 내에서 공격과 방어를 실행할 수 있도록 개발하였다. 센서모듈과 출력 기능을 각 모듈별로 설계하였으며, 각각의 모듈은 Serial 통신을 통해 연동할 수 있고, IoT 보안 교육에 적합하도록 노트북, PC와 같은 대중적 장비에 의해 프로그래밍이 가능하도록 설계하였다.

4. 결론

본 연구에서 개발된 해커보드는 이중 MCU 특징을 갖는다. 또한, 해커보드를 구성하는 각종 센서를 모듈화하여 그 기능별로 구성하는 필요한 교육과정에 맞추어 교육환경을 구성할 수 있도록 개발하였으며, 이후 확장성을 고려하여 설계하였다.

본 논문에서는 해커보드의 설계전략을 8가지로 세분화하여 수립하였으며, 이것이 해커보드의 하드웨어 설계에 어떻게 반영되었는지 제시하였다. 또한, 설계 구현된 모듈에 대하여 하드웨어 설계 결과 및 기능사양과 교육을 위한 실습 시나리오를 제시하였다. 구체적으로는 MCU, PCB, 회로도, 센서모듈을 포함하여

설명함으로써, IoT 보안 교육용 하드웨어 설계의 참고가 될 수 있도록 하였다. 향후에는 실 환경에서 교육용 하드웨어를 활용한 결과, 교육만족도 및 피드백, 기존 교육과의 차이점 등을 비교 분석하여 설계에 반영하고, 이중 MCU를 활용한 IoT 보안 교육용 하드웨어를 구현할 필요가 있다. 또한, 실 환경에 적용하여 보다 효과적이고 효율적인 하드웨어 설계로 개선하고 실제 교육 현장 적용에 따른 효과성을 연구하여야 한다.

본 연구를 통해 IoT보안 교육이 이론 중심이 아닌 물리적인 하드웨어 교구를 활용함으로써 교육에 대한 호감을 키우고, 1개의 보드 내에서 공격과 방어를 실습하는 있는 보안 교육환경을 간단하게 구성할 수 있을 것으로 기대한다.

참고문헌

[1] E.Y.Oh, M.Y.Yoon, S.H.Lee, J.J.Yoon, J.Y.Lee, Y.J.Lee, “Current Status and Prospects of Hyper-Connected Urban Societies Urban Information Service”, No.407, p.3, 2016.

[2] WEF(World Economic Forum) https://www.weforum.org/events/annual-meeting-of-the-gl obal-future-councils-2023

[3] National Informatization White Paper(2014) National Information Society Agency(NIA).

[4] J.E. Kim. "An Analysis of the effect of Artificial Intelligence on Human Society", The Journal of the Convergence on Culture Technology (JCCT), 5(2), pp.177-182, 2019. http://dx.doi.org/10.17703/JCCT. 2019.5.2.

[5] Seo, B, EduTech, and “A place called schoo”, Proceedings of the Korean Society For The Study Of Sociology Of Education, pp.59-82, 2021.

[6] Back, S., Jo, S., Kim, N., & Choi, M., Noh, K, “A study on the application of EduTech for multi-cultural people”, Journal of Digital Convergence, 14(3), pp.55-62, 2016.

[7] Yoon, H, “A study on Edu-tech activation methods for learners in university eucation”, The Journal of Humanities and Social science, 13(1), pp.3135-3148, 2022.

[8] Kim, S, “In the digital big data classroom reality and application of smart education : learner-centered education using edutech”, Journal of the Korea Entertainment Industry Association, 5(4), pp.279-286, 2021.

[9] Nam, S, “Development and application for edu-tech based flipped learning”, The journal of human-ities and social sciences 21, 11(3), pp.1677-1692, 2020.

[10] Park, J., & Gil, J, “Edutech in the era of the 4th industrial revolution”, KIPS Transactions on Software and Data Engineering, 9(11), pp.329-331, 2020.

[11] 강호원, “2023년 제3호_영국 초중등학교의 EdTech 활용 현황과 시사점", 교육현안보고서, 2023.

[12] 이호건, "한국 ICT 기반 교육 서비스의 신남방 국가 진출을 위한 주력 국가의 에듀테크 시장 분석" 통상정보연구 21(4), pp.237-256, 2019.

[13] 배영임, 신혜리. “코로나 19, 언택트 사회를 가속화하다", 이슈 & 진단, pp.1-26, 2020.

[14] 이숙윤, 유길상, “ARM Cortex-M4 를 활용한 사물인터넷 센서의 통신 플랫폼 구현", 한국컴퓨터교육학회 학술발표대회논문집, 25(1), (A), pp.283-285, 2021.

[15] 배점한, 김종태, “IoT Things 를 위한, 설계변경이 용이한 실용적 HW/SW 설계 방법", 한국통신학회논문지, 44(6), pp.1193-1200, 2019.

〔저자소개〕

김 동 원 (Dong-Won Kim)
2009년 2월 서울과학기술대학교 학사
2012년 2월 건국대학교 석사
2021년 2월 고려대학교 박사
2017년~현재 건양대학교 스마트보안학과 교수
email : blast@konyang.ac.kr