사이버 물리 시스템 보안 프로젝트 제안서

범죄 예방을 위한 미허가 출입 탐지/대응 모델:

중앙대학교 310관 적용 예시

2조

20161569 최경식

20165545 조현우

20165079 김영빈

목차

1. 주제 선정 계기

(1) 지금까지는 건물 내에서 중요한 자원이 물리적으로 위치하지 않는 호실의 경우, 미 허가 출입은 예방을 중심으로. 일정 시간을 주기로 순찰하거나 하는 가벼운 경비만으로 진행되어 왔다. 하지만 IoT 기술의 발전이 진행되면서, 방마다 비치된 에어컨과 같은 기기들도 악의적인 공격자에게 공격 루트를 제공할 수 있는 노드가 되었다. 따라서 평범한 호실이더라도 특정 업무를 위해 사용되지 않을 때에는 허가되지 않은 출입을 방지해야 할 필요성이 늘어났다.

(2) 이를 위하여 건물 내 이상 상황 탐지를 위한 지표를 설정하고, 프로세스 모델을 확립하여 조사 및 분석 대상의 범위를 좁혀주게 된다면 (전 구역 → 이상 상황이 탐지된 구역) 더 효율적인 보안이 가능할 것이라고 결론을 내렸다.

(3) 이에 대학생이라는 신분에서 지켜야할 보안의 대상이 무엇이 될 수 있을까를 고민하던 중 중앙대학교 310관 건물 자체에 대해 관심을 갖게 되었다. 310관은 많은 학생들이 실제로 이용을 하며 비인가자(외부인, 배달부, 택배직원 등)의 접근 역시 쉬운 편이다. 이 프로젝트를 진행하면서 실제로 이상 상황 탐지 기술을 중앙대학교 강의실에 접목시켜, 원래는 비어 있어야 할 강의실에 누군가가 접근하는 상황을 **이상 상황**으로 정하여 보안조치 대상(강의실)을 특정해보려 한다.

310관 전경

2. 프로젝트 목표 및 수행 효과

1. 사이버 물리 보안 시스템의 근간을 이루는 센서의 탐지 데이터를 자세하게 공부하고 실제로 활용해볼 수 있다.
2. 실습 시간에 학습한 웹 크롤링과 파이썬에서 제공하는 기능들을 학습해 데이터를 정제해볼 수 있다..
3. 기존의 물리 시스템에 모델링을 적용하여 보안 강화에 기여할 수 있다.

3. 미허가 출입 대응 프로세스

1. 건물의 각 호실 사용 계획을 정리하여 저장한다
2. 탐지 센서를 통하여 각 건물 별 현재 사용되고 있다고 예상되는 강의실을 파악한다.
    - 사용자 존재여부를 파악할 수 있는 외부조건을 정한다. (모션 감지 등)
3. 정리된 현 시점 호실 실제 사용현황을 파일로 저장한다.
4. 각 호실 사용 계획 데이터와 현 시점 실제 사용 데이터를 비교한다.
5. 서로 다른 부분을 비인가된 출입, 즉 이상 상황으로 판단하고 조치를 취한다.

4. 파일럿 테스팅: 310관

구분	건물명	호실	호실명
강의실	310관(100주년기념관)	B603	대형강의실
강의실	310관(100주년기념관)	B602	대형강의실
강의실	310관(100주년기념관)	B601	대형강의실
강의실	310관(100주년기념관)	B502	대형강의실
강의실	310관(100주년기념관)	B501	대형강의실
심장제세동기	310관(100주년기념관)	B4F	AED심장제세동기(통합상황실)
행정실	310관(100주년기념관)	B415	종합방재센터
편의시설	310관(100주년기념관)	B414	학생편의시설(우편물분류실)
편의시설	310관(100주년기념관)	B413	학생편의시설(우편취급국)
편의시설	310관(100주년기념관)	B412	학생편의시설(헤어샵)
편의시설	310관(100주년기념관)	B411	학생편의시설(편의점)
편의시설	310관(100주년기념관)	B410	학생편의시설(복사점)

파일럿 테스팅은 크게 다음 세 가지로 수행된다.

1. 강의실 사용 계획 파악하고 DB화
2. DB데이터와 센서 데이터 접목을 통한 해당 시점 실제 강의실 사용 현황 파악
3. 이상 데이터 식별 시, 데이터 분석을 통한 관리자 알림

4. 1.사용 툴

Python	데이터 크롤링, 서버 구축
Excel	데이터 정제
Github	버전 관리
AWS	서버 관리
Gmail	이상 식별 결과 출력

4.2. 강의실 사용 계획 파악

우선 아래의 방법으로 학교 내부의 강의실 사용 현황을 수집한다. 내부 강의실 사용 현황을 파악할 때 수업시간에 진행했던 파이썬 크롤링 기법을 이용할 계획이다.

1. 학교 포탈 사이트에 존재하는 강의 계획서를 모두 크롤링하여, 시간표와 강의실, 위치 데이터를 구해온다.
2. 중앙대학교 홈페이지에서 각 건물에 존재하는 모든 호실 정보에 접근하여, 이 중에서 강의실의 목적으로 사용되는 곳을 크롤링한다.
3. 1과 2에서 구한 데이터를 이용하여, 각 강의실마다 수업 시간표를 구한다.

각 강의실마다 수업 시간표를 구할 때, 기존의 크롤링 한 메타 데이터들을 프로젝트에서 사용 가능한 형태로 바꾸어주는 과정이 필요하다. 각 프로세스에서 필요한 파이썬 기능들을 실습을 통해 추가로 공부하고 구현해보면서 파이썬에 대한 이해도를 높일 수 있다.

4.3. 실제 강의실 사용 현황 파악

위 4.1. 에서 얻은 자료와 사용자가 있다는 현실적인 정보를 종합하면 실질적 강의실 사용 현황을 파악이 가능하다. 사용자가 있다는 현실적인 데이터를 추출할 외부 요인들의 예시로는 아래와 같다. 이때, 외부 요인 데이터는 310관의 실제 데이터를 이용한다면 좋겠지만 현 코로나 19 사태로 학교 강의실에 대한 접근이 불가능하고, 실제 데이터의 수집 가능 여부도 알 수 없다. 프로젝트를 진행하면서 최대한 실제 데이터를 얻도록 노력할 계획이지만, 불가능하다면 아두이노 센서를 구매하여 코딩을 통해 직접 센서를 만들어 볼 계획이다. 직접 센서를 만들어보고 데이터를 서버로 전송 받는 프로세스를 구현해보면서 실제 센서 데이터가 전달되는 형태와 센서가 특정 상황을 어떻게 인식하는지를 공부할 기회를 가질 수 있다.

외부 요인	설명
전력 사용량 탐지	전력 사용량이 기준을 초과하면 강의실이 사용 중이라고 판단 및 신호 전송
모션 감지 센서	움직임이 인식될 때마다 신호를 전송
형광등 온도 감지 센서	형광등의 발열 정도에 따라 온도를 감지하여 신호 전송

전력 사용량은 해당 강의실이 비어있을 때의 평균 전력을 측정하여 적절한 기준으로 정한 뒤, 특정 시간마다 수집되는 전력 데이터를 설정한 기준과 비교해서 이상 상황을 탐지 한다. 스마트 그리드, EMS(Energy Management System)에서 받아올 수 있다. 아래는 전력 사용량을 표시한 예시이다.

전력 사용량 예시

외부 요인 중 모션 감지 센서와 온도 감지 센서의 경우 아두이노 기반 센서를 사용한 시뮬레이션이 가능하다. 해당 제품을 구매하여 실제 데이터를 받아오는 과정을 진행해본다.

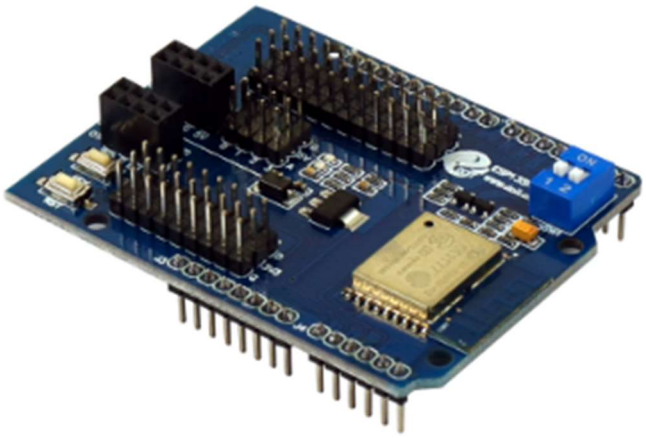
아두이노 모션 감지 센서

아두이노 온도 감지 센서

```
int ledPin = 9;       //  LED 핀
int inputPin = 7;     // 센서 신호핀
int pirState = LOW;   // 센서 초기상태는 움직임이 없음을 가정
int val = 0;          // 센서 신호의 판별을 위한 변수

void setup(){
    pinMode(ledPin, OUTPUT);    // LED를 출력으로 설정
    pinMode(inputPin, INPUT);    // 센서 Input 설정
    Serial.begin(9600);         // 시리얼 통신, 속도는 9600
}

void loop(){
  val = digitalRead(inputPin);          // 센서 신호값을 읽어와서 val에 저장

  if (val == HIGH) {                    // 센서 신호값이 HIGH면(인체 감지가 되면)
    digitalWrite(ledPin, HIGH);        // LED ON
    if (pirState == LOW){
         Serial.println("Welcome!");    // 시리얼 모니터 출력
         pirState = HIGH;
    }
   }
    else {                              // 센서 신호값이 LOW면(인체감지가 없으면)
    digitalWrite(ledPin, LOW);         // LED OFF
   if (pirState == HIGH){
        Serial.println("Good Bye~");   // 시리얼 모니터 출력
        pirState = LOW;
    }
  }
}
```

코딩 예시

아두이노 센서를 각 강의실에 설치한 후, 모션 감지와 온도 감지 결과를 코딩을 통해 지속적으로 서버에서 입력값을 받도록 한다.



아두이노 웹 서버 보드

센서 아두이노의 경우, 센서를 통해 하드웨어에서 어떠한 처리를 할 수는 있지만, 이러한 처리 연산과정이 데이터로써 서버로 전송이 되지 않기 때문에 웹 서버보드를 통해 웹 소켓과 연결하여 데이터를 받아오도록 한다. 웹 소켓과 연결할 땐 이더넷 보드를 통해 노트북과 연결하여 설정을 먼저 해주고, 이후에 노트북에서 이용중인 와이파이 IP쪽으로 데이터를 보내 데이터를 전달받을 수 있도록 할 예정이다. 이러한 과정이 기존에 알고 있던 프로그래밍 언어로는 구현할 수 없기 때문에, 아두이노 언어를 익히고, 코딩 스타일을 익혀야 한다. 또 아두이노 보드에 어떠한 저항값과 어떠한 케이블을 연결할 지 등, 센서의 Physical Layer에 대한 새로운 학습이 필요하다.

프로젝트 구현 과정에서 예상되는 문제점으로는 다음과 같이 두 가지가 존재한다.

1. 모션 센서와 온도 센서의 데이터 처리방법을 둘 다 익히기는 프로젝트의 기간 상 무리가 있다.
2. 웹 서버로 데이터를 보내기 위해서는 웹 서버 메인보드, 센서 메인보드와 같이 부품을 여러 개 구매해야 하는데 비용이 많이 든다.

이러한 이유로 모션 센서를 위주로 파일럿 테스팅을 진행할 예정이다.

4.4. 미허가 출입 탐지

1. 센서를 통해 현재 강의실을 실시간으로 감지하고, 지속적으로 강의실의 데이터를 받아오도록 한다.
2. 강의실 상태 데이터가 기준을 초과할 경우, AWS API gateway를 통해 이벤트를 발생시키고, AWS Lambda에서 DynamoDB에 저장된 계획 데이터를 호출하고, 이 때 가져온 데이터를 현재의 강의실 상태 데이터와 비교하여, 이상 상황인지 정상 상황인지를 파악한다.
3. 이상 상황이라고 인식되면, AWS Lambda를 통해 관리자 알림 API를 호출하고, 관리자에게 알림을 보내는 Lambda함수를 새로 구현하여, 관리자 Gmail API에 이벤트를 발생시키도록 한다. 마지막으로 이러한 이상 상황이라고 식별된 위치 데이터를 관리자에게 현재 시간과 위치를 내용으로 하는 메일을 보내도록 한다.

5. 발전 방안

1. 예외 상황에 대한 적용이 필요하다.

   (ex. 강의가 휴강 되었거나 연장되는 경우, 강의가 진행되는 호실이 바뀐 경우)

   - 학교 측에서 데이터 입력의 형식을 정해주고, 이를 강의 계획서 강의 계획 파트에 업데이트하도록 한다면, 좀 더 쉽게 데이터 활용이 가능할 것이다
2. 본 프로젝트를 진행하면서 사용할 데이터들을 학교측에 제안을 해서 꾸준하게 데이터를 제공받을 수 있다면 이 프로그램의 실사용이 가능해질 것이다.
3. 직관적인 UI와 시각화를 통해 인원에게 미허가 출입이 일어난 강의실을 보여줄 수 있다면 효율적이고 빠른 대처가 가능해질 것이다.
4. 다양하게 센서의 종류를 두고, Data Logger를 이용한다면 더욱 다양한 데이터를 얻을 수 있고 이러한 데이터를 바탕으로 더 신뢰성있는 모델을 제시할 수 있다.