2023-2학기 DU-도전학기 계획서

<table>
<tr><td>과제명</td><td colspan="4">AI 기반, 홈 IoT 기기를 향한 DRDoS 공격 탐지 솔루션 개발</td></tr>
<tr><td>신청 유형</td><td colspan="4">☐ 개인 ■ 팀(팀명: NetDuS)</td></tr>
<tr><td>도전 영역</td><td colspan="4">■ 전공(주전공 또는 복수전공) ☐ 일반선택</td></tr>
<tr><td>신청 학점</td><td colspan="4">3학점</td></tr>
<tr><td rowspan="5">참여자</td><td>성명</td><td>소속</td><td>학번</td><td>비고</td></tr>
<tr><td>김[redacted]</td><td>컴퓨터공학전공</td><td rowspan="4">[redacted]</td><td>팀장</td></tr>
<tr><td>이[redacted]</td><td>컴퓨터공학전공</td><td>팀원</td></tr>
<tr><td>박[redacted]</td><td>컴퓨터공학전공</td><td>팀원</td></tr>
<tr><td>안[redacted]</td><td>컴퓨터소프트웨어전공</td><td>팀원</td></tr>
<tr><td>지도교수 의견</td><td colspan="4">상기 학생 중, [redacted] 학생은 도전학기 경험자로서 매우 적극적이고 성실한 태도로 우수한 결과를 도출한 학생들입니다. 두 학생이 처음 도전학기에 도전하는 [redacted] 학생에게 모범을 보이며 팀을 잘 이끌 것이라 생각합니다. 학생들이 도전학기를 통해 수업시간에 배운 사물인터넷, 정보보호, 인공지능을 심화학습하며 전공 실력을 향상시킬 수 있을 것이라 기대하고, 학생들이 성공적으로 도전학기를 수행할 수 있도록 옆에서 성심껏 지도하겠습니다.

(소속) 컴퓨터공학전공 (성명) 김지연 (서명 또는 날인)</td></tr>
</table>

1. 도전 배경

사물인터넷은 각종 사물에 센서와 통신 기능을 내장하여 인터넷에 연결하는 기술로 무선 통신을 통해 각종 사물을 연결하는 기술을 의미한다. 오늘날, 실생활에서 사물인터넷 기기들이 보편화되면서 개인정보유출이나 홈 캠 해킹 등 보안 취약점이 증가하고 있는 추세이다. 실제로 한국 인터넷진흥원에서 발표한 사물인터넷 관련 보안 취약점 신고 현황에 따르면 2015년부터 2020년까지 신고 건수는 1,701건으로 2018년 신고 건수인 2015(130건) 대비 3년 사이 약 2.9배 증가한 것을 알 수 있다.[1] 만약 사물인터넷 기기들이 사이버 공격에 노출 될 경우 사회적 혼란 및 2차 범죄로 확산 될 우려가 있기에 사물인터넷 기기들에 대한 사이버 공격을 탐지하고 대응할 수 있는 솔루션이 필요해졌다. 이에 따라, 본 팀은 다양한 사물인터넷 기기 중 실생활에서 보편화된 홈 IoT에 대한 **사이버 공격 및 탐지 솔루션**을 연구하고자 한다. 먼저 가용성 공격과 스위치 재밍 공격 등과 같이 홈 IoT 기기들의 정보를 탈취하거나 마비시킬 수 있는 강력한 공격들 중 DRDoS에 대해 조사를 수행하고 홈 IoT 테스트 베드를 구축할 계획이다. 이후에는 홈 IoT의 정상 패턴들과 사이버 공격을 받았을 때의 비정상 패턴들을 학습 데이터 셋으로 구축한 뒤, 사이버 공격이 들어왔을 경우, 네트워크의 정상/비정상 패턴을 탐지할 수 있도록 수집한 데이터셋 인공지능 모델에 학습시켜 **홈 IoT 공격을 탐지하는 솔루션 개발**에 도전해 보려고 한다.

[1] 정용철,2021.08.25.,"월패드 망분리'홈IoT 첫 보안규정만든다" 전자신문 https://www.etnews.com/20210825000174

2. 도전 과제의 목표

가. 팀 목표

본 팀의 목표는 홈 IoT에서 사용되는 센서의 정상 패턴과 사이버 공격이 주입되었을 때의 비정상 패턴을 수집하여 IoT 기기의 정상/비정상 상태를 탐지할 수 있는 인공지능 모델을 개발하는 것이다. 먼저 미세먼지 센서나 온습도 센서 등의 홈 IoT에서 사용되는 센서들을 라즈베리파이에 각각 연결하여 IoT 환경을 구축하여 센싱 데이터를 대시보드로 확인할 수 있도록 할 것이며, 센서들의 정상 패턴과 사이버 공격을 주입한 비정상 패턴들을 수집하여 학습 데이터셋을 구축하려고 한다. 이때, 비정상 패턴 수집 시 **오탐률**을 줄이기 위해 사이버 공격의 강도를 상, 중, 하로 나누어 공격을 수행할 예정이다. 이후에는 수집한 학습 데이터셋으로 학습을 진행하여 **홈 IoT 센서들의 정상/비정상 상태를 탐지**할 수 있는 인공지능 모델을 개발하려고 한다.

나. 개인 목표

1) 홈 IoT 기기에 대한 공격 데이터 수집 및 비교 분석과 정상/비정상 상태 탐지 인공지능 모델링 (김진경)

- 홈 IoT 기기들에 대한 DRDoS 공격 조사 및 주입 진행
- IoT 기기들에 대한 패턴 및 비교 분석을 수행하면서 공격 탐지를 위한 공격 강도별 인공지능 학습 데이터 셋 구성
- 그라파나 대시보드에서 공격을 주입했을 경우 공격을 알려주는 기능 제작을 진행하면서 전공역량 강화

2) 홈 IoT 환경 제작 및 코딩과 IoT 기기들에 대한 데이터 수집과 그라파나 (Grafana) 대시보드 구현 (이현우)

- IoT 기기들에 대한 패턴 비교 분석을 수행하면서 정상 상태 학습을 위한 강도별 인공지능 학습 데이터셋 구성
- 라즈베리 파이를 이용한 홈 IoT 기기 환경 제작 및 코딩
- 그라파나를 이용한 IoT 기기 데이터 대시보드 구현 및 IoT 기기들의 공격 강도별 상태 시각화 구현을 진행하며 전공 역량 강화

3) 홈 IoT 기기에 대한 공격 데이터 수집 및 비교 분석과 정상/비정상 상태 탐지 인공지능 모델링 (박은영)

- 홈 IoT 기기들에 대한 DRDoS 공격 조사 및 주입 진행
- IoT 기기들에 대한 패턴 및 비교 분석을 수행하면서 공격 탐지를 위한 공격 강도별 인공지능 학습 데이터 셋 구성
- 그라파나 대시보드에서 공격을 주입했을 경우 공격을 알려주는 기능 제작을 진행하면서 전공역량 강화

4) 홈 IoT 환경 제작 및 코딩과 IoT 기기들에 대한 데이터 수집과 그라파나 (Grafana) 대시보드 구현 (안동휘)

- IoT 기기들에 대한 패턴 비교 분석을 수행하면서 정상 상태 학습을 위한 강도별 인공지능 학습 데이터셋 구성
- 라즈베리파이를 이용한 홈 IoT 기기 환경 제작 및 코딩
- 그라파나를 이용한 IoT 기기 데이터 대시보드 구현 및 IoT 기기들의 공격 강도별 상태 시각화 구현을 진행하며 전공 역량 강화

3. 도전 과제 내용

가. 홈 IoT 취약점 및 사이버 공격 조사

홈 IoT는 기존의 사물인터넷을 스마트홈에 접목하여 모바일 기기, 가전 등을 인터넷과 통신으

로 모두 연결하여 정보를 수집하고 교환하는 플랫폼을 의미한다. 이를 통해 집 밖에서 스마트 기기를 사용하여 집 안의 연결된 모든 사물들을 제어하고 통제할 수 있는 기술이지만 인터넷에 연결된 물건들이 해커의 공격 대상이 된다면 사생활 침해, 개인정보 유출 등의 문제로 발전할 가능성이 존재한다. 홈 IoT에 대한 대표적인 사이버 공격으로는 공유기 장악 공격이 있으며 이 공격은 인터넷에 연결된 공유기 자체의 취약점을 찾거나 보안 수준이 낮은 관리자 비밀번호를 통해 공유기의 제어권을 탈취하고 모든 연결된 디바이스의 제어권을 얻어서 문을 마음대로 여는 등의 각종 물리적 범죄 행위가 일어날 수 있다. 마찬가지로 카메라가 있는 장비의 제어권을 얻게 된다면 일종의 실시간 몰래카메라로 작동할 수 있다.

<표 1> IoT 보안 취약점 신고 건수

나. 인공지능 제작 및 학습 데이터 수집

'인공지능'이란 사람의 사고나 학습을 컴퓨터가 수행할 수 있게 하는 기술로 음성 및 작성된 언어, 이미지 등의 자료를 이해하고 번역하거나 데이터를 분석하고 분류 및 추천하는 기능을 포함하여 다양한 고급 기능을 수행할 수 있는 기술이다. 인공지능을 학습시키기 위해 반드시 필요한 과정은 데이터 셋을 구축하는 것이다. 이때, 학습 데이터 셋은 인공지능이 특정 사물을 인지할 수 있도록 도와주는 여러 가지 정보가 담긴 데이터 셋을 의미하며, 성능을 향상시키기 위해서는 양질의 데이터 셋이 필요하게 된다. 본 팀은 정확도를 높이기 위한 정상/비정상 상태 탐지 인공지능을 제작하기 위해 정상/비정상 학습 데이터 셋을 강도별로 나누어 수집할 것이며, IoT를 향한 사이버 공격이 수행될 경우, 정상/비정상 상태를 탐지할 수 있는 인공지능 모델을 개발하려고 한다.

라. 업무 분장 내용

팀원 성명	소속	담당 업무
[redacted]	컴퓨터공학전공	- 홈 IoT 기기들에 대한 DRDoS 공격 조사 및 주입 진행 - IoT 기기들에 대한 패턴 및 비교 분석을 수행하면서 공격 탐지를 위한 DR-DoS 공격 강도별 인공지능 학습 데이터 셋 구성 - 그라파나 대시보드에서 공격을 주입했을 경우 공격을 알려주는 기능 제작을 진행하면서 전공역량 강화
[redacted]	컴퓨터공학전공	- 홈 IoT 기기들에 대한 패턴 비교 분석을 수행하면서 정상 상태 학습을 위한 강도별 인공지능 학습 데이터셋 구성 - 라즈베리 파이를 이용한 홈 IoT 기기 환경 제작 및 코딩 - 그라파나를 이용한 IoT 기기 데이터 대시보드 구현 및 IoT 기기들의 공격 강도별 상태 시각화 구현을 진행하며 전공 역량 강화

[redacted]	컴퓨터공학전공	- 홈 IoT 기기들에 대한 DRDoS 공격 조사 및 주입 진행 - IoT 기기들에 대한 패턴 및 비교 분석을 수행하면서 공격 탐지를 위한 DRDoS 공격 강도별 인공지능 학습 데이터 셋 구성 - 그라파나 대시보드에서 공격을 주입했을 경우 공격을 알려주는 기능 제작을 진행하면서 전공역량 강화
[redacted]	컴퓨터소프트웨어 전공	- 홈 IoT 기기들에 대한 패턴 비교 분석을 수행하면서 정상 상태 학습을 위한 강도별 인공지능 학습 데이터셋 구성 - 라즈베리파이를 이용한 홈 IoT 기기 환경 제작 및 코딩 - 그라파나를 이용한 IoT 기기 데이터 대시보드 구현 및 IoT 기기들의 공격 강도별 상태 시각화 구현을 진행하며 전공 역량 강화

4. 도전 과제 추진일정

주차	활동 목표	활동 내용	투입 시간
1주차	실험 환경 구축 및 시나리오 제작	김[redacted] 팀장) : IoT 기반 사이버 공격 조사	9시간
		이[redacted] 팀원) : 홈 IoT 기기 환경 제작	8시간
		박[redacted] 팀원) : IoT 기반 사이버 공격 조사	10시간
		안[redacted] 팀원) : 홈 IoT 기기 환경 제작	8시간
2주차	실험 환경 구축 및 시나리오 제작	김[redacted] 팀장) : IoT 기반 DRDoS 공격 조사	8시간
		이[redacted] 팀원) : 홈 IoT 기기 환경 제작	10시간
		박[redacted] 팀원) : IoT 기반 DRDoS 공격 조사	8시간
		안[redacted] 팀원) : 홈 IoT 기기 환경 제작	10시간
3주차	실험 환경 구축 및 시나리오 제작	김[redacted] 팀장) : DRDoS 공격 시나리오 작성 및 조사	8시간
		이[redacted] 팀원) : 홈 IoT 기기 코딩	10시간
		박[redacted] 팀원) : DRDoS 공격 시나리오 작성 및 조사	8시간
		안[redacted] 팀원) : 홈 IoT 기기 코딩	10시간
4주차	구축 환경 테스트 및 공격 조사	김[redacted] 팀장) : DRDoS 공격 시나리오 작성 및 조사	6시간
		이[redacted] 팀원) : 홈 IoT 기기 코딩	6시간
		박[redacted] 팀원) : DRDoS 공격 시나리오 작성 및 조사	6시간
		안[redacted] 팀원) : 홈 IoT 기기 코딩	6시간
5주차	IoT 정상 및 공격 데이터 수집	김[redacted] 팀장) : IoT를 향한 DRDoS 공격 데이터 수집	6시간
		이[redacted] 팀원) : IoT 기기들의 정상 데이터 수집	5시간
		박[redacted] 팀원) : IoT를 향한 DRDoS 공격 데이터 수집	5시간
		안[redacted] 팀원) : IoT 기기들의 정상 데이터 수집	5시간
6주차	그라파나를 이용한 IoT 기기 대시보드 구축	김[redacted] 팀장) : IoT를 향한 DRDoS 공격 데이터 수집	5시간
		이[redacted] 팀원) : IoT 기기들의 정상 데이터 수집	4시간
		박[redacted] 팀원) : IoT를 향한 DRDoS 공격 데이터 수집	5시간
		안[redacted] 팀원) : IoT 기기들의 정상 데이터 수집	4시간
7주차	그라파나를 이용한 IoT 기기 대시보드 구축	김[redacted] 팀장) : 정상 및 공격 데이터 비교 분석	5시간
		이[redacted] 팀원) : IoT 기기 데이터 대시보드 구축	5시간
		박[redacted] 팀원) : 정상 및 공격 데이터 비교 분석	5시간
		안[redacted] 팀원) : IoT 기기 데이터 대시보드 구축	5시간
8주차	중간 보고서 작성	김[redacted] 팀장) : 중간 보고서 작성	5시간
		이[redacted] 팀원) : 중간 보고서 작성	5시간
		박[redacted] 팀원) : 중간 보고서 작성	5시간
		안[redacted] 팀원) : 중간 보고서 작성	5시간
9주차	정상/비정상 탐지 인공지능 모델링 조사 및 제작 진행	김[redacted] 팀장) : 인공지능 모델 조사 및 공부	6시간
		이[redacted] 팀원) : 인공지능 모델 조사 및 공부	6시간
		박[redacted] 팀원) : 인공지능 모델 조사 및 공부	6시간
		안[redacted] 팀원) : 인공지능 모델 조사 및 공부	6시간
10주차	정상/비정상 탐지 인공지능 모델링 제작 진행	김[redacted] 팀장) : 인공지능 모델링 및 제작	6시간
		이[redacted] 팀원) : 학습 데이터 분석 및 검증	6시간
		박[redacted] 팀원) : 인공지능 모델링 및 제작	6시간
		안[redacted] 팀원) : 학습 데이터 분석 및 검증	6시간

11주차	정상/비정상 탐지 인공지능 정상 모델 학습 및 검증	김	팀장) : 인공지능 모델 제작	7시간
		이	팀원) : 정상 학습 데이터 주입	7시간
			팀원) : 인공지능 모델 제작	7시간
			팀원) : 정상 학습 데이터 주입	7시간
12주차	정상/비정상 탐지 인공지능 공격 모델 학습 및 제작	김	팀장) : 인공지능 모델 제작	5시간
		이	팀원) : 비정상 학습 데이터 주입	4시간
			팀원) : 인공지능 모델 제작	5시간
			팀원) : 비정상 학습 데이터 주입	4시간
13주차	인공지능 모델 성능 검증	김	팀장) : 인공지능 모델 성능 검증 진행	6시간
		이	팀원) : 인공지능 모델 성능 검증 진행	6시간
			팀원) : 인공지능 모델 성능 검증 진행	6시간
			팀원) : 인공지능 모델 성능 검증 진행	6시간
14주차	인공지능 모델 성능 검증 및 유지보수 수행	김	팀장) : 인공지능 모델 유지보수	5시간
		이	팀원) : 인공지능 모델 성능 재검증	5시간
			팀원) : 인공지능 모델 유지보수	5시간
			팀원) : 인공지능 모델 성능 재검증	5시간
15주차	최종 보고서 작성	김	팀장) : 최종 보고서 작성	3시간
		이	팀원) : 최종 보고서 작성	3시간
			팀원) : 최종 보고서 작성	3시간
			팀원) : 최종 보고서 작성	3시간

5. 활동 지원비 상세 내역

활동 지원비 신청내역			
항 목		산출근거	금액(원)
재료비		- 라즈베리 홈 IoT 키트 131,000원 - 라즈베리 파이4B – 8GB 115,000원	246,000원
자료구입비		- 마이크로비트 & 아두이노 홈 IoT 키트 교재 16,200원 - 파이썬 머신러닝 정복하기 18,000원	34,200원
회의비		- 회의비 8,600원 × 4명 × 15주 = 516,000원	516,000원
등록비		- 대한임베디드공학회 100,000원 × 4명 = 400,000원	400,000원
교통비		- 동대구-부산 왕복 KTX - 38,000원(왕복) × 4명 × 1회 = 152,000원 - 대구 - 제주도 왕복 항공권 - 150,000 × 4 명 × 1회 = 600,000원	752,000원
인쇄비	학술대회 포스터 제작비	- A1, 2장 분량 - A+ 인쇄소 기준 견적 가격	50,000원
합계(원)			**1,998,200원**

6. 과제 수행 후 제출할 수 있는 결과물

도전 학기 활동은 수행하면서 제출할 수 있는 결과물로는 팀 공통 결과물이 있다. 팀 공통 결과물은 홈 IoT 센싱 데이터 및 상태를 대시보드로 보여줄 수 있도록 할 것이며, 이를 기반으로 DRDoS 공격이 들어왔을 경우, 홈 IoT 기기들의 정상/비정상 상태을 탐지하여 피드백(알림)을 제공하는 모델이 될 것이다. 그리고 제작한 정상/비정상 상태 탐지 인공지능 모델을 중심으로 학술대회 논문을 작성하여 2023 한국 임베디드 공학회에 참여하고자 한다.

가. 팀 공통 결과물 : 홈 IoT 기기들이 사이버 공격을 받았을 경우 정상/비정상 상태를 탐지할 수 있는 인공지능 모델, 학술대회 논문