2024학년도 2학기 강의계획안

교과목명	AI기반IoT보안	개설전공	인공지능 · 소프트웨어학부	면담시간	
학수번호-분반	G18461-01	시간	3.0	학점	3.0
교수명	김종길		연구실	진선미 225호	
연락처			E-MAIL	jongkil@ewha.ac.kr	
역량			주제어		

1. 교과목 개요 Course Description

본 과목에서는 네트워크와 연결되는 모든 기기들을 뜻하는 Internet-of-Things (IoT) 및 이를 관리하기 위한 클라우드 시스템에 대한 보안 위협 및 이에 대한 해결방법을 탐구한다. 특히, AI 기반의 프라이버시 보호 방법과 AI로 인한 위협을 탐구하여, AI가 IoT 및 클라우드 시스템에 미치는 영향에 대해 탐구하고자 한다.

2. 선수학습사항 Prerequisites

사이버 보안 또는 AI관련 지식. (필수 사항은 아님)

3. 강의방식 Course Format

강의 Lecture	발표/토론 Discussion/Presentation	실험/실습 Experiment/Practicum	현장실습 Field Study	기타 Other
80%	20%	0%	0%	0%

- 강의 진행 방식 설명 (explanation of course format):

4. 교과목표 Course Objectives

본 과목은 학생들에게 다음의 역량을 향상시킴을 목표로 한다.
- IoT 시스템의 특징과 구조를 이해한다.
- IoT 시스템이 가지는 보안 위험을 설명할 수 있다.
- 안전한 IoT 시스템을 위한 AI 기술을 설명할 수 있다.
- IoT 시스템을 위협하는 AI 공격 방법을 설명할 수 있다.

5. 학습평가방식 Evaluation System

*

중간고사 Midterm Exam	기말고사 Final Exam	퀴즈 Quizzes	발표 Presentation	프로젝트 Projects	과제물 Assignments	참여도 Participation	기타 Other
0%	50%	0%	10%	20%	20%	0%	0%

* 그룹 프로젝트 수행 시 팀원평가(PEER EVALUATION)이 평가항목에 포함됨.
  Evaluation of group projects may include peer evaluations.

- 평가방식 설명 (explanation of evaluation system):

본 과목의 수강생은 1개의 프로젝트와 1~2개의 과제물을 수업을 기간동안 수행해야 한다.
프로젝트는 중간, 최종 발표 및 리포트로 이루어져 있으며, 과제물은 별도의 발표를 수행하지 않음.

6. 주교재 Required Materials

해당사항없음.

7. 부교재 Supplementary Materials

해당사항없음.

8. 참고문헌 Optional Additional Readings

수업을 통해 전달될 계획임.

9. 강의내용 Lecture contents

주별	날짜	주요강의내용 및 자료, 과제
제 1 주	2024/09/06(금)	Introduction to IoT and Cloud systems
제 2 주	2024/09/13(금)	Threats on IoT and Cloud
제 3 주	2024/09/20(금)	Data Security on IoT and Cloud
제 4 주	2024/09/27(금)	IoT Application Security on IoT and Cloud (1)
제 5 주	2024/10/04(금)	IoT Application Security on IoT and Cloud (2)
제 6 주	2024/10/11(금)	IoT Infrastructure Security on IoT and Cloud
제 7 주	2024/10/18(금)	Privacy-preserving Techniques for IoT (1)
제 8 주	2024/10/25(금)	Privacy-preserving Techniques for IoT (2)
제 9 주	2024/11/01(금)	Privacy-preserving Techniques for IoT (3)
제 10 주	2024/11/08(금)	Project Presentation (I)
제 11 주	2024/11/15(금)	Adversarial Techniques for IoT(1)
제 12 주	2024/11/22(금)	Adversarial Techniques for IoT (2)
제 13 주	2024/11/29(금)	Adversarial Techniques for IoT (3)
제 14 주	2024/12/06(금)	Project Presentation (II)
제 15 주	2024/12/13(금)	Final Exam

10. 수업운영규정 Course Policies

* 실험, 실습실 진행 교과목 수강생은 본교에서 진행되는 법정 '실험실안전교육(온라인과정)'을 필수로 이수하여야 함.

11. 참고사항 Special Accommodations

* 학적 제57조에 의거하여 장애학생은 학기 첫 주에 교과목 담당교수와의 면담을 통해 출석, 강의, 과제 및 시험에 관한 교수학습지원 사항을 요청할 수 있으며 요청된 사항에 대해 담당교수 또는 장애학생지원센터를 통해 지원받을 수 있습니다.

*** 강의계획안의 내용은 추후 변경될 수 있습니다.**