

# 바삭 마이낙

MSc. 소프트웨어 | AI 연구원 | GenAI 취약점 분석가

+82 10-5462-5888 | [mainak.basak101@gmail.com](mailto:mainak.basak101@gmail.com) | [GitHub](#) | [포트폴리오](#)

## 연구 요약

AI 보안, 네트워크 보안, 이상 탐지, 보안 데이터 마이닝, 설명 가능한 AI, 생성적 적대 모델, 데이터 분석을 위한 기계학습 모델 및 지도/비지도 데이터 모델 분류 모델 생성 분야에서 5년 이상의 경험을 보유한 AI 연구원. 현재 연구 관심사는 악성코드 탐지 시스템 모델링, 트랜스포머 (어텐션) 모델, 대규모 언어 모델 (LLM)의 취약점 및 프롬프트 주입 공격 탐색에 있음.

## 학력

박사 학위(2025년 7월 졸업 예정)

컴퓨팅학부, GPA: 4.3/4.5.

**논문** - 적응형 다중 모달 AI를 활용한 견고한 사이버 위협 탐지: 교차 확산 그래프부터 동적 잔차 비전 네트워크까지(아직 제출되지 않음).

공학 석사

가천대학교, 대한민국

2019년 9월-2022년 2월

IT 융합공학과, GPA: 4.2/4.5

**논문** - 밀집 연결 잔여 인볼루션 네트워크를 통한 잠재 특성 시각화를 통한 악성코드 적대자 설명. [\[link\]](#)

공학 학사

MCKV 공과대학, 콜카타, 인도

2013년 9월 - 2017년 9월

자동차공학과, GPA: 6.69

**프로젝트** - 상용 유틸리티 차량 새시 최적화

2022 - 현재

가천대학교, 대한민국

## 전문 경력

연구 조교 및 실험실 강사

AI 보안 연구실

- AI 보안 및 딥러닝 개념에 대한 강의 제공
- 학습 자료 준비, 과제 할당 및 학부생 지도
- Python 및 PyTorch에 대한 실습 교육 제공
- 다양한 트랜스포머 모델 개발
- 직무 관련 행정 업무 수행

2022년 2월 - 현재.

AI 소프트웨어학과, 가천대학교, 대한민국.

AI 보안 연구원

AI 정보보안(IS) 연구실

- 여러 프로젝트의 엄격한 기한을 충족하기 위한 연구 프로세스 간소화
- 리더십 팀과 협력하여 관련 질문을 식별하고 최적의 수집 방법 결정
- 데이터 분석 결과를 해석하여 추론 및 결론 도출
- AI 보안, DL 설명 가능한 AI 및 네트워크 보안에 관한 연구 논문, 보고서 및 요약본 작성
- 패턴 및 동향 분석 및 해석
- 대상 데이터 연구, 수집 및 보고서 준비에 대한 정확한 정량적 분석 수행
- 프로젝트 계획 또는 검토 또는 기술 지원을 제공하기 위해 과학자, 엔지니어 또는 다른 사람들과 회의
- 최신 문헌을 파악하고 더 전략적인 연구 결정을 내리기 위해 기술 및 전문 출판물 및 저널 검토
- 전문 분야에서 자체 연구 수행

2019년 9월- 2022년 2월.

가천대학교, 대한민국.

졸업생 견습생, 기술 엔지니어

Piaggio Vehicles Pvt. Ltd., 이탈리아 회사.

- 담당: AutoCad-Catia-OHSAS 18001-HIRA-6Sigma-5S-ISO TS 16949-ISO 14001-2004-Excel
- 회사 자산 분석 및 관리에 참여
- 입찰, 보고서, 세미나 등 여러 행정 업무 수행

2016년 9월- 2017년 5월

푸네, 인도.

## 출판물

### 학술지

1. 바삭 마이낙, 김동욱, 한명목, 신건윤, "조밀 모듈 지식 그래프 생성을 통한 지식 추출을 위한 설명 가능한 침입 탐지 프레임워크", *IEEE Transactions on Information Forensics and Security* (심사 중) (영향력 지수: 6.3, Q1).
2. 바삭 마이낙, 김동욱, 한명목, 신건윤, "X-GANet: 견고한 네트워크 침입 탐지를 위한 설명 가능한 그래프 기반 프레임워크", *Applied Sciences* 2025, (수락 완료) (영향력 지수: 2.7, Q2).
3. 바삭 마이낙, 김동욱, 한명목, 신건윤, "동적 잔차 커널 네트워크를 통한 잠재 특징 시각화를 이용한 어텐션 기반 악성코드 탐지 모델", *Sensors*, 2024, 24, 7953 (출판 완료). (영향력 지수: 3.97, Q1).
4. 바삭 마이낙, 한명목, "CyberSentinel: 중요 운영 환경에서의 악성코드 탐지를 위한 투명한 방어 프레임워크", *Sensors*, 2024, 24, 3406 (출판 완료) (영향력 지수: 3.97, Q1).
5. Safarov Furkat, 바삭 마이낙, 라시드 나시모프, Akmalbek Abdusalomov, 조영임, "네트워크 기반 IoT 공격 탐지를 위한 설명 가능한 경량 블록 어텐션 모듈 프레임워크", *Future Internet*, 15(9), 297 (2023) (영향력 지수: 3.0, Q2).
6. 윤지영, 바삭 마이낙, 한명목, "Attention-가이드 프로토타입을 활용한 시스템 로그의 해석 가능한 이상 탐지", *Knowledge-Based Systems*, Elsevier (출판 완료, 2020) (영향력 지수: 8.038, Q1).
7. 윤지영, 바삭 마이낙, 한명목, "COVID-19 환자의 해석 가능한 사망률 분류를 위한 베이지안 규칙 모델링", *Computers, Materials & Continua*, 2021, 69(3), 2827-2843 (출판 완료, 2021) (영향력 지수: 3.860, Q1).

### 학술대회

1. 바삭 마이낙 and 한명목, "DCBAM - Explainable Lightweight Framework for Network-Based IOT Attack Detection", *Proceedings of KIIS Autumn Conference 2023 Vol. 32, No. 2* (H5 인덱스: 157).
2. 바삭 마이낙, 윤지영 and 한명목, "Depth Point Attention Guided Network for Automatic Classification of COVID-19 From CT Images", *KSII (한국인터넷정보학회) 추계학술대회 2020, 2020년 8월* (H5 인덱스: 197).

### Thesis

1. 조밀하게 연결된 잔차 인벌루션 네트워크를 활용한 잠재 특징 시각화를 통한 악성코드 행위 설명. [\[링크\]](#)

## 프로젝트

- 한국연구재단(NRF) 한국 정부(MSIT) 지원 연구비 (No. NRF-2022R1F1A107337513)
- **MeetMinder** — 지능형 회의 일정 관리를 위한 AI 기반 폴스택 웹 애플리케이션. 대규모 언어 모델(LLM)을 활용하여 사용자 입력을 이해하고, 최적의 시간을 제안하며, 스마트 요약본을 생성함.
- 원격 데스크톱 프로토콜의 횡적 이동에서 보안 침해를 위한 커널 알고리즘 및 노드 감지 알고리즘 개발, MSIT(과학기술정보통신부, IITP-2021-2020-0-01602), 대한민국.
- 프로젝트: 대규모 언어 모델의 프롬프트 주입 공격 탐지 및 완화  
설명: 프롬프트 기반 취약점 탐색, 자동화된 탐지 메커니즘 설계 및 의도하지 않은 모델 응답을 방지하기 위한 필터링 기술 개발.
- 대학원 연구 지원 프로젝트 (GCU-2019-2019-0777), 대한민국.
- 공인 데이터 처리 전문가 (AMCAT 라이선스: 2806504-211)
- **Experthub** 기술 개발 센터, 푸네. 최신 자동차 공학 도구에 대한 집중 교육 프로그램.  
작업: 자동화 및 시뮬레이션 소프트웨어(CAD, CAM, DWS, 로봇공학).
- 프로젝트: 프리랜서 스타트업 및 NGO 웹사이트 관리  
내용: 다양한 웹 개발 프로젝트 및 콘텐츠 관리.

## 기술

언어	Python, C++, MATLAB, Java.
도구/라이브러리	NumPy, SciPy, OpenCV, Matplotlib/Seaborn, Pandas, Scikit-Learn.
프레임워크	PyTorch, TensorFlow, Keras.

## 추천인

[요청 시 제공 가능합니다.](#)