MAINAK BASAK

MSc. Software | AI Researcher | GenAI Vulnerability Analyst

☎ +82 10-5462-5888 ✉ mainak.basak101@gmail.com GitHub Portfolio

RESEARCH SUMMARY

AI researcher with 5+ years of experience in AI security, network security, anomaly detection, secure data mining, explainable AI, generative adversarial models, machine learning models on data analysis and creating of classification models on supervised and unsupervised data-models. Current research interests lie in modeling malware detection systems, transformer (attention) models, explored vulnerabilities and prompt injection attacks in large language models (LLMs).

EDUCATION

Doctorate of Philosophy PhD (to be graduated on July 2025) **2022 — Present**

THESIS - Adaptive Multimodal AI for Robust Cyber-Threat Detection: From Cross-Diffused Graphs to Dynamic Residual Vision Networks. (Not yet submitted).
4.3/4.5, School of Computing,
Gachon University, South Korea (Republic of Korea).

Master of Engineering **Sep 2019 — Feb 2022**

THESIS – Explaining malware adversary by visualizing latent features through densely connected residual involution network. [link]
4.2/4.5, Dept. of IT Convergence Engineering,
Gachon University, South Korea (Republic of Korea).

Bachelor of Engineering **Sep 2013 – Sep 2017**

Project – Optimization of Chassis of Commercial Utility Vehicle.
GPA 6.69, Dept. of Automotive Engineering, MCKV Institute of Engineering, Kolkata, India.

PROFESSIONAL EXPERIENCE

Research Assistant and Lab Instructor **Feb 2022 – Present**

AI Security Lab *Dept. of AI Software, Gachon University, Rep. of Korea.*

- Provided lectures on the concepts of AI Security and deep learning.
- Prepared course materials allocated tasks and supervised undergrad students.
- Provided hands-on training on Python and PyTorch.
- Developed various Transformer models.
- Conducted job-related administrative works.

AI Security Researcher **Sep 2019 — Feb 2022**

AI Information Security (IS) Lab *Gachon University, Rep. of Korea.*

- Streamlined research processes to meet tight deadlines for multiple projects.
- Collaborated with leadership team to identify relevant questions and determine best methods of collection.
- Interpreted data analysis results to draw inferences and conclusions.
- Wrote research papers, reports and summaries regarding **AI Security and DL Explainable AI and Network Security**.
- Analyzed and interpreted patterns and trends.
- Performed accurate quantitative analysis of targeted data research, collection and report preparation.
- Conferred with scientists, engineers or others to plan or review projects or to provide technical assistance.
- Reviewed technical and professional publications and journals to stay current on recent literature and make more strategic research decisions.
- Conducted own research in field of expertise.
- Learned new laboratory techniques and applied expertise in carrying out enhanced experiments under supervision of senior lab members.

Graduate Apprentice Trainee, Warranty Technical Engineer **Sep 2016 — May 2017**

Piaggio Vehicles Pvt. Ltd., Italy. *Pune, India.*

- Responsibility: AutoCad-Catia-OHSAS 18001-HIRA-6Sigma-5S-ISO TS 16949-ISO 14001-2004-Excel
- Participated in analyzing and managing company assets.
- Performed several administrative duties such bidding, reports, seminars etc.

Publication

Journals

1. **Mainak Basak**, Dong-Wook Kim, Myung-Mook Han and Gun-Yoon Shin, “Explainable Intrusion Detection Framework for Knowledge Extraction from Dense Module Knowledge Graph Generation”, IEEE Transactions on Information Forensics and Security (*Under review*) (SCI/*Impact factor: 6.3, Q1*).
2. **Mainak Basak**; Kim, D.-W.; Han, M.-M.; Shin, G.-Y. X-GANet: An Explainable Graph-Based Framework for Robust Network Intrusion Detection. *Appl. Sci.* 2025, *15*, 5002. (SCIE/*Impact factor: 2.7, Q2*).
3. **Mainak Basak**, Dong-Wook Kim, Myung-Mook Han and Gun-Yoon Shin, “Attention-Based Malware Detection Model by Visualizing Latent Features Through Dynamic Residual Kernel Network”. *Sensors 2024*, 24, 7953. (SCIE/*Impact factor: 3.97, Q1*).
4. **Mainak Basak**, Myung-Mook Han, " CyberSentinel: A Transparent Defense Framework for Malware Detection in High-Stakes Operational Environments", Sensors **2024**, *24*, 3406. (SCIE/*Impact factor: 3.97, Q1*).
5. Safarov Furkat, **Mainak Basak**, Rashid Nasimov, Akmalbek Abdusalomov, and Young Im Cho. 2023. "Explainable Lightweight Block Attention Module Framework for Network-Based IoT Attack Detection" *Future Internet* 15, no. 9: 297. (Impact factor: 3.0, Q2).
6. Jiyoung Yun, **Mainak Basak** and Myung-Mook Han, " Interpretable Anomlay Detection in System Logs Using Attention-guided Prototypes ", Knowledge-Based Systems, Elsevier, Published, 2020. (SCI/Impact factor: 8.038, Q1).
7. Jiyoung Yun, **Mainak Basak** and Myung-Mook Han, “Bayesian Rule Modeling for Interpretable Mortality Classification of COVID-19 Patients”, Computers, Materials & Continua 2021, 69(3), 2827-2843, Published, 2021(SCIE/Impact factor: 3.860, Q1).

Conferences

1. **Mainak Basak** and Myung-Mook Han, "DCBAM - Explainable Lightweight Framework for Network-Based IOT Attack Detection ", Proceedings of KIIS Autumn Conference 2023 Vol. 32, No. 2 (H5 index: 157).
2. **Mainak Basak**, Jiyoung Yun and Myung-Mook Han, "Depth Point Attention Guided Network for Automatic Classification of COVID-19 From CT Images", KSII (Korean Society for Internet Information) Fall Conference 2020, Aug. 2020 (H5 index: 197).

Thesis

1. Explaining malware adversary by visualizing latent features through densely connected residual involution network. [link]

Projects

- National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT)(No. NRF-2022R1F1A107337513)
- (SAAS) MeetMinder — An AI-powered full-stack web application for intelligent meeting scheduling and management. Leverages large language models (LLMs) to understand user input, suggest optimal times, and generate smart summaries.
- Development of kernel Algorithm and Node Detection Algorithm for security breaches in Lateral Movement in Remote Desktop Protocol, MSIT (Ministry of Science and ICT, IITP-2021-2020-0-01602), Rep. of Korea.
- GitProject: *Detecting and Mitigating Prompt Injection Attacks in Large Language Models*

  Description: Explored prompt-based vulnerabilities, designed automated detection mechanisms, and developed filtering techniques to prevent unintended model responses.
- Graduate School Research Funding Project (GCU-2019-2019-0777), Rep. of Korea.
- Certified Data Processing Specialist (AMCAT License: 2806504-211)
- Experthub Skill Development Center, Pune. Intensive training program on latest Automotive Engineering Tools.
  Worked on: Automation & Simulation Software (CAD,CAM,DWS,Robotics).
- Project: Freelance Startup & NGO website management.
  Content: Various web development projects & content management.

Skills

Languages	Python, C++, MATLAB, Java.
Tools/Libraries	NumPy, SciPy, OpenCV, Matplotlib/Seaborn, Pandas, Scikit-Learn.
Frameworks	PyTorch, TensorFlow, Keras.

References

Available upon request.✉