Haoyang Hu

: hhyoffer@163.com | : https://github.com/ALIENHHY | : https://alienhhy.github.io/

Education

- **The University of Hong Kong (HKU) [🌐]** *Sept. 2025 - Dec. 2026*
  M.Sc in Computer Science, will enroll in Fall 2025. Hong Kong, China
- **Nanjing University of Science and Technology (NJUST) [🌐]** *Sept. 2021 - Jun. 2025*
  *B.Eng in Cyberspace Security, supervised by **Prof. Zhichao Lian**.* Wuxi, China
  - GPA: 85.25/100, rank top 12%, [Link-to-My-Transcripts]

Patents and Publications

C=Conference, J=Journal, P=Patent, A=Other Articles

[C.1] Yican Geng∗, **Haoyang Hu**∗, Zhaoxuan Ge and Zhichao Lian. ***Network Intrusion Detection Algorithm Based on LightGBM Model and Improved Particle Swarm Optimization***. In 2024 IEEE Cyber Science and Technology Congress (CyberSciTech), DOI: 10.1109/CyberSciTech64112.2024.00021

[P.1] Chanying Huang, Changji Yao, **Haoyang Hu**, Kedong Yan. ***News recommendation method and system based on national secret algorithm and federated learning***. CN118094008A, Pending.

[P.2] **Haoyang Hu**. ***A Guide Cane and its Control Method***. CN111110531A, Active.

[P.3] **Haoyang Hu**. ***A Guide Cane***. CN212235240U, Active.

[A.1] **Haoyang Hu** and Zhen Peng. ***ESG Risks and Opportunities in the Development of Artificial Intelligence***. Knowledge Management, Tencent, Dec. 2024.

[A.2] **Haoyang Hu** and Zhen Peng. ***Observations on the Global Governance Landscape of Artificial Intelligence Governance***. Knowledge Management, Tencent, Nov. 2024. (Awarded as **'KM Good Article'**)

* *: These authors contributed equally to this work.*

Projects

Partial List

- **Threat Analysis Research on Large-Scale Text Models: Attack Toolkit for LLMs** *Nov. 2024 - Current*
  - Focusing on pioneering advanced jailbreaking attacks tailored for Chinese language models, optimizing algorithms like TAP and PAIR for efficient and semantically coherent adversarial prompt generation.
  - Improve attack strategies so that attacks can work on complex environments such as Chinese language models.
  - Developing a specialized toolkit for analyzing jailbreaking attacks on text-based large models, aimed at advancing understanding and capabilities in model security research and providing insights for defense strategies.
- **AISDR: An Study on AI-Based Technologies for Drug Registration Assistance** *Jun. 2024 - Current*
  - Pioneered the industry's first quantifiable pharmaceutical registration framework by collecting datasets.
  - Utilized LLMs for feature selection and employed Random Forest models for phase-based forecasting.
  - Applied other machine learning algorithms to predict final outcomes from constructed time series datasets, alongside designing a recommendation trigger to offer improvement suggestions in case of prediction failures.
- **OptiCrow: Research and Development of an IoT Network Intrusion Detection System** *Feb. 2024 - Sept. 2024*
  - Optimized LightGBM hyperparameters using Genetic Algorithms (GA) and Particle Swarm Optimization (PSO), significantly improving the efficiency and accuracy of IDS for predicting network intrusion traffic.
  - Applied advanced strategies like Levy flight to enhance the global search capabilities of the CSA algorithm.
  - Introduced binary conversion to improve global search ability and computational efficiency in the EHO algorithm.
  - Our preliminary work has been accepted by CyberSciTech 2024, currently drafting a follow-up paper!
- **Efficient-FedRec-SM: News Recommendation System Based on Federated Learning and SM** *Sept. 2023 - Jan. 2024*
  - Developed and implemented cryptographic solutions using SM2 and SM9 algorithms to ensure secure and integrity-protected transmission of gradient data in federated learning frameworks.
  - Decrypted received data on the server to verify the integrity and accuracy of the uploaded gradient data.
  - Awarded third prize in the National Cryptography Competition and pended a patent!
- **SafeGuide: Intelligent Guide Cane Based on Computer Vision** *Sept. 2018 - Dec. 2023*
  - Developed a multifunctional intelligent cane using Python and Arduino programming, incorporating features like intelligent recognition and obstacle avoidance using advanced algorithms such as time difference and FFT.
  - Integrated the YOLO algorithm and micro camera to enable visual functionality, enhancing the cane's ability to accurately perceive and respond to its surroundings.
  - Awarded one invention patent, one utility model patent, and received multiple awards in various competitions!

Work Experiences

- **Nanjing Nebulorix Co., Ltd.** *Nov. 2024 - Current*
  Co-Founder Nanjing, China
- **Tencent [🌐]** *Sept. 2024 - Dec. 2024*
  Intern, ESG Coordination Office (ECO Lab), mentored by senior expert Elmer Peng Shenzhen, China
  - Exploring AI governance, cybersecurity and privacy protection:
    - **Industry insights and research:** Conducted in-depth research on AI governance, cybersecurity and privacy protection, analyzing industry trends and peer strategies of relevant companies.
    - **Data analysis and reporting:** Contributed to the collection, analysis, and visualization of ESG data, assisted in drafting analytical reports, and supported data-driven decision-making.**[AI in ESG] [AI Governance]**
  - Developing AI-driven efficiency tools:
    - **Daily News Reporting System:** Developed a workflow to automatically gather and select news on relevant topics, generate a report and deliver it to colleagues' mailboxes, which is already in operation.
    - **Writing Agent:** Built a proprietary knowledge base for training, designed specialized prompts, and developed a agent tailored for ESG report writing, which is set to be deployed in our team.
    - **Computer Vision Recognition:** Deployed an image recognition model for the 'Emin Environmental Protection Action Group' mini program using ResNet and OCR to identify bike, ebike, bus and other images. The mini program has been successfully launched and registered by over 5,000 colleagues. **[Code]**
- **China Telecom [🌐]** *Jan. 2024 - Feb. 2024*
  Intern, Cloud Network Maintenance Center Quzhou, China
- **CINGHOO Technology Co., Ltd. [🌐]** *Jul. 2023 - Aug. 2023*
  Intern, Judicial Appraisal Institute Chengdu, China
- **MoreSec Technology Co., Ltd. [🌐]** *Jul. 2022 - Aug. 2022*
  Intern, DarkArmor Lab Hangzhou, China

Honours and Awards

Selected Awards

- **Competition Awards**
  - First Prize, *National College Student Data Analysis Competition*, Online *Dec. 2023*
  - Third Prize, *National Cryptography Technology Competition*, Urumqi, China *Nov. 2023*
  - Third Prize, *"TIPDM CUP" Data Mining Challenge*, Online *Jun. 2023*
- **School Honours**
  - First Prize, Outstanding Student Scholarship, NJUST (Top 4%) *Sept. 2024 & Apr. 2024*
  - Success Scholarship, NJUST *Sept. 2024*
  - Outstanding Class Cadre, NJUST (1/70) *Sept. 2024 & Apr. 2024*
  - Beyond Scholarship, NJUST *Mar. 2024*
  - Merit Student, NJUST (6/70) *Nov. 2023*
  - Third Prize, Outstanding Student Scholarship, NJUST (Top 15%) *Sept. 2023 & Mar. 2023 & Sept. 2022*

Panorama

Partial List

- **Students' Activities**
  - Student Congress, NJUST *Mar. 2024 - Current*
    - Permanent Representatives
  - Major of 2021 in Cyberspace Security, NJUST *Sept. 2021 - Current*
    - Secretary of the Reunion Branch
  - Basketball & Badminton Team of the School of Cyberspace Security, NJUST *Sept. 2021 - Current*
    - Team Member
  - Summer Social Practice Activity (Provincial Core Project) *Jul. 2023 & Jul. 2022*
    - Team Leader
- **Certifications**
  - Advanced Certified Data Analyst, China Financial Analysis Institute *Feb. 2024*
  - Junior Industrial Internet platform development engineer, Talent Exchange Centre of MIIT *Jun. 2023*
  - VRC Spin Up Head Referee Certification, REC Foundation *Apr. 2023*
  - Judge Certification, REC Foundation *Apr. 2023*
- **Robotics**
  I have participated in 8 seasons of VEX-EDR (now known as VEX-V5 [🌐]) robotics competitions since elementary school.
  - Second Runner-up, *RoboCom World Robotics Competition Final*, Beijing, China *Aug. 2018*
  - Runner-up, *National VEX Robotics Engineering Challenge*, Xian, China *Aug. 2016*
  - Glod Award, *VEX World Championship*, Louisville, USA [🌐] *Apr. 2016*
  - Glod Award, *Asia-Pacific Robotics Championship*, Melbourne, Australia [🌐] *Dec. 2015*
  - Champion, *National VEX Robotics Engineering Challenge*, Weihai, China *Aug. 2015*