Canterbury
CT1 1DS
United Kingdom
✉ *ae455@kent.ac.uk*
in *adelelzemity*
adelsamir.com

Adel Samir ElZemity

Professional Summary

Doctoral Researcher in Computer Science at the University of Kent, UK, with a background as a software engineer. Research focuses on the safety and security of Large Language Models (LLMs) and their applications in cyber security. Passionate about AI and quickly adapts to new frameworks and technologies. Particularly excited about advancing AI safety and security.

Education

2023–Present **PhD in Computer Science**, *University of Kent*, United Kingdom
- Focus on AI safety and cyber security
- Full-Merit scholarship

2018–2023 **Bachelor's of Science in Computer Engineering**, *Nile University*, Egypt
- GPA (3.9/4.0) with Honors (President's List, Dean's List)
- Full Merit Scholarship

2021 **Exchange Semester (Global UGRAD)**, *Fayetteville State University*, USA
- GPA (4.00/4.00) with Honors (President's List)
- Full-Merit scholarship

2021 **Exchange Semester (Erasmus+)**, *Riga Technical University*, Latvia
- GPA (4.00/4.00) with Honors (President's List)
- Full-Merit scholarship

Work Experience

2023–Present **Doctoral Researcher**, *University of Kent*, United Kingdom
- Leading research on LLM safety and security, developing evaluation frameworks to assess risks in fine-tuned models
- Building machine learning pipelines to train and evaluate LLMs on cyber security tasks, with focus on safety alignment
- Part of the "Countering HArms caused by Ransomware on the Internet of Things (CHARIOT)" project funded by EPSRC in the UK

2023–Present **Teaching Assistant**, *University of Kent*, United Kingdom
- Teaching assistant for undergraduate and postgraduate courses in Computer Science
- Supporting students in programming, algorithms, and software development
- Conducting lab sessions and providing academic guidance

2022–2023 **Machine Learning Engineer**, *National Cancer Research Center*, Spain
- Tested and optimised supervised ML models to detect metal binding sites in proteomes
- Participated in the UniProt Machine Learning challenge 2022
- Created python pipeline for exploring, cleaning, and filtering datasets to improve accuracy and efficiency

2021–2022 **Software Engineer**, *Intelligent Systems Lab (ISL)*, USA
- Applied expertise in deep learning to design and implement an architecture for robot's ZED Camera
- Improved efficiency of object detection on the moon by 2%
- Configured 24 Linux-based robots using RaspberryPi and Jetson Nano using ROS and Python

Publications

2025 **Analysing Safety Risks in LLMs Fine-Tuned with Pseudo-Malicious Cyber Security Data**, *ArXiv*
Adel ElZemity, Budi Arief, Shujun Li

2025 **CyberLLMInstruct: A New Dataset for Analysing Safety of Fine-Tuned LLMs Using Cyber Security Data**, *ArXiv*
Adel ElZemity, Budi Arief, Shujun Li

2024 **Privacy Threats and Countermeasures in Federated Learning for Internet of Things**, *IEEE iThings*
Adel ElZemity, Budi Arief

2023 **A Comparative Analysis of Time Series Transformers and Alternative Deep Learning Models for SSVEP Classification**, *International Conference on Model and Data Engineering*
Heba Ali, Adel ElZemity, Amir E Oghostinos, Sahar Selim

2023 **A Transformer-Based Deep Learning Architecture for Accurate Intracranial Hemorrhage Detection and Classification**, *IEEE 3ICT*
ElZemity et al.

2020 **Wastewater Treatment Model with Smart Irrigation Utilizing PID Control**, *IEEE NILES*
ElZemity et al.

2019 **Interfacial Modification of Perovskite Solar Cell Using ZnO Electron Injection Layer with PDMS as Antireflective Coating**, *IEEE NILES*
Mohamed K. Othman, Adel ElZemity, Mohamed K. Rawash, Hazem A. Taha, Shorouk Alalem, Maryam El-Fdaly, Yasser M. El-Batawy

Technical Skills

Development & Tools

Python, Shell, HTML, CSS, JavaScript, SQL, TypeScript, Swift, Flutter, React, Next.js, WordPress, VSCode, Cursor, Terminal, XCode, PyCharm, Google Colab, Kaggle, Hugging Face, LaTeX, Markdown, Word, Excel, PowerPoint, PDF, Overleaf, AWS, Azure, GCP, Vercel, GitHub Pages, Cloudflare, Git, GitHub, GitLab, Jupyter Notebook, Docker, Kubernetes, Virtual Machines, Virtualization, Linux, Windows, MacOS, API, REST, Webhooks, WebSockets, CI/CD, DevOps, Cloud Computing, Cloud Infrastructure, Data Science, Data Engineering, Data Analysis, Data Visualization

Artificial Intelligence

Machine Learning, Deep Learning, Computer Vision, Natural Language Processing, Time Series Analysis, Fine-tuning LLMs, Retrieval-Augmented Generation (RAG), Federated Learning, Federated Learning for IoT, Flower framework, TensorFlow, PyTorch, Keras, Scikit-learn, Pandas, NumPy, Matplotlib, Seaborn, ChatGPT, Claude, Gemini, Llama, Qwen, Mistral, Gemma, DeepSeek

Cyber Security

Network architecture & security (TCP/IP, VLANs, routing, switching, VPNs), IoT Security (LoRaWAN, Thread, Zigbee, Bluetooth, Wi-Fi), Access control systems (RFID, NFC, Biometrics), Capture the Flag (CTF), Malware analysis (Malware, Ransomware, Botnet), AI Security, attacks, and defenses (LLM, RAG, Federated Learning), Privacy and Data Protection (GDPR, CCPA, HIPAA), Encryption and Decryption (AES, RSA, SHA)

Languages

Arabic (Native), English (Fluent), German (Intermediate)