Adel ElZemity

ae455@kent.ac.uk +44 740 590 6591 Canterbury, CT1 1DS Linkedin GitHub

EDUCATION

Ph.D. in Computer Science 2023 – present | Canterbury, UK
University of Kent
Research focus: Security of Large Language Models (LLMs)

Bachelor's of Science in Computer Engineering 2018 – 2023 | Giza, Egypt
Nile University
GPA: 3.9/4.0 | Honors: President's List, Dean's List | Full Scholarship

WORK EXPERIENCE

Cybersecurity Researcher Sep 2023 – present | Canterbury, UK
- Led the development of anomaly detection pipeline using ML to detect ransomware attacks in IoT.
- Created real and simulated testbeds with Thread Protocol and Contiki-NG to analyse network traffic and perform deep packet inspection.
- This work is part of the "Countering HArms caused by Ransomware on the Internet of Things (CHARIOT)" project funded by EPSRC in the UK.

Machine Learning Engineer Jan 2022 – May 2023 | Madrid, Spain
National Cancer Research Center
- Tested and optimised supervised ML models to detect metal binding sites in proteomes under the supervision of Dr. Michael Tress and Dr. Fernando Pozo.
- Participated in the UniProt Machine Learning challenge 2022 by creating a python pipeline for exploring, cleaning, and filtering datasets to improve accuracy and efficiency.

Software Engineer Aug 2021 – Jan 2022 | Fayetteville, NC, USA
Intelligent Systems Lab (ISL)
- Applied expertise in deep learning to design and implement an architecture that effectively segmented the live feed of the robot's ZED Camera, improving the efficiency of object detection on the moon by 2%.
- Configured 24 Linux-based robots using RaspberryPi and Jetson Nano using (Robot Operating System) ROS and Python.

PROJECTS & SKILLS

CyberLLMInstruct – Dataset Development and Safety Evaluation for Cyber Security LLM Fine-Tuning Sep 2024 – Apr 2025
Skills: Large Language Model (LLM) fine-tuning, adversarial testing, model safety evaluation, cyber security dataset creation, data preprocessing, prompt engineering, AI ethics and responsible AI, security benchmarking (OWASP Top 10, CyberMetric), vulnerability assessment, threat intelligence analysis, malware and phishing simulation, zero-day and injection attack analysis, secure AI development, performance optimisation, high-performance computing (HPC) with NVIDIA A100 GPUs, mixed-precision training, AdamW optimisation, Transformers, TRL, and PyTorch frameworks, DeepEval, garak, GPT-4 and Gemini integration, automated classification and labelling, reproducible research, quantitative model evaluation, security risk analysis, dataset documentation and version control (GitHub), research writing and publication (ACM AISec '25).

Privacy Threats and Countermeasures in Federated Learning for Internet of Things – A Systematic Literature Review Sep 2023 – Sep 2024

Skills: Systematic literature review (SLR), PRISMA protocol application, academic database searching (Scopus, IEEE Xplore, ACM, Wiley, ScienceDirect), research question formulation, inclusion and exclusion criteria design, data collection and synthesis, literature analysis and classification, taxonomy development, privacy threat modelling, defensive measure evaluation, federated learning (FL), Internet of Things (IoT) security, privacy-preserving machine learning, differential privacy, secure multi-party computation (SMPC), encryption and obfuscation techniques, noise injection, blockchain integration, data anonymisation, quantitative metric comparison, research gap identification, academic writing, result visualisation, and peer-reviewed publication (IEEE 2024).

Protein Binding Site Prediction Using Machine Learning (Bind-Predict-ML) Jan 2022 – May 2023

Skills: UniProt data exploration, sequence-based binding site prediction, data cleaning and wrangling, dataset construction, feature engineering, exploratory data analysis (EDA), Jupyter notebooks, deep learning pipeline development, metal ion binding site prediction, model training and evaluation, hyperparameter tuning, Python, machine learning theory application, automated data processing, reproducible research workflows, Git version control, bioinformatics sequence processing, classification modelling, performance benchmarking, result annotation and documentation.

RELEVANT PUBLICATIONS

Analysing Safety Risks in LLMs Fine-Tuned with Pseudo-Malicious Cyber Security Data
SECAI 2025 (International Workshop on Security and Artificial Intelligence), a workshop co-located with ESORICS 2025 (30th European Symposium on Research in Computer Security)
Adel ElZemity, Budi Arief and Shujun Li

CyberLLMInstruct: A Pseudo-Malicious Dataset Revealing Safety-Performance Trade-offs in Cyber Security LLM Fine-tuning
AISec 2025 (18th ACM Workshop on Artificial Intelligence and Security), a workshop co-located with ACM CCS 2025 (32nd ACM Conference on Computer and Communications Security)
Adel ElZemity, Budi Arief and Shujun Li

Privacy Threats and Countermeasures in Federated Learning for Internet of Things: A Systematic Review
Adel ElZemity, and Budi Arief *In 2024 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics* , 2024

A Transformer-Based Deep Learning Architecture for Accurate Intracranial Hemorrhage Detection and Classification
Heba Ali, ***Adel ElZemity***, Amir E Oghostinos , and 1 more author
In International Conference on Model and Data Engineering , 2023

A Comparative Analysis of Time Series Transformers and Alternative Deep Learning Models for SSVEP Classification
Ali, H., **ElZemity, A.**, Oghostinos, A. E., & Selim, S. (2023, November). In International Conference on Model and Data Engineering (pp. 3-16). Cham: Springer Nature Switzerland.

Wastewater Treatment Model with Smart Irrigation Utilizing PID Control
A. ELZemity et al. 2020 2nd Novel Intelligent and Leading Emerging Sciences Conference (NILES)pp. 374-379, doi: 10.1109/NILES50944.2020.9257882

Interfacial Modification of Perovskite Solar Cell Using ZnO Electron Injection Layer with PDMS as Antireflective Coating
M. K. Othman et al. 2019 Novel Intelligent and Leading Emerging Sciences Conference (NILES) pp. 209-213, doi: 10.1109/NILES.2019.8909336.

LANGUAGES

Arabic ●●●●● English ●●●●●

German ●●●○○