PETRAS Lenses: Securing the Edge, Useful, Useable Decentralisation
PETRAS Sectors: Ambient Environments, Transport and Mobility

José Cano (University of Glasgow)
Jeremy Singer (University of Glasgow)
Sye Loong Keoh (University of Glasgow)
Ferheen Ayaz (University of Glasgow)
Christos Stylianou (University of Glasgow)
Danilo Pau (STMicroelectronics)
Mounia Kharbouche-Harrari (STMicroelectronics)

Multimodal AI-based Security at the Edge (MAISE)

Introduction

MAISE is a co-optimisation strategy balancing:

AI Model Optimisation → Robustness → Continuous and secure Deployment

Motivation

- Multi-modal systems have multiple object, speech and text recognition capabilities

- AI models are prone to attacks
- AI for small IoT devices is in demand

Aims & Objectives

- Optimised AI models: < 2 MB
- Secure

Methodology

Deployable Models

TFLite, OpenVIN

Adversarial Defence

Input transformation, Architectural defence, Adversarial training

Continuous and secure deployment

Encryption

Key Findings

Benchmark Models	Size	Format
Kws CNN	3.4 MB	TFLite
Mobilenet V2 Quant	3.7 MB	OpenVINO
SSD Mobilenet V2 Quant	6.2 MB	TFLite

- Models are not optimised for small devices, i.e. <2 MB
- Not secure

Publications

i. J. Turner, J. Cano, V. Radu, E. J. Crowley, M. O'Boyleand A. Storkey, "Characterising Across-Stack Optimisations for Deep Convolutional Neural Networks," *IEEE International Symposium on Workload Characterization (IISWC)*, 2018.
ii. H. C. Tan, K. Lim, S. L. Keoh, Z. Tang, D. Leong andC. S. Sum, "Chameleon: A blind double trapdoorhash function for securing AMI data aggregation," *IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, 2018.
iii. D. Pau, M. Lattuada, F. Loro, A. De Vita and G.Domenico Licciardo, "Comparing Industry Frameworks with Deeply Quantized Neural Networks on Microcontrollers," *IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, 2021.

PETRAS THE PETRAS NATIONAL CENTRE OF EXCELLENCE FOR IoT SYSTEMS CYBERSECURITY
UKRI UK Research and Innovation
University of Glasgow
life.augmented
sicsa* The Scottish Informatics & Computer Science Alliance