University of Messina, Italy
Department of Mathematical and Computer Sciences,
Physical Sciences and Earth Sciences

Subject: Internship Proposal

ID	PTI_EN_Villari Massimo_19/03/2026 8.10.09
Data	19/03/2026 8.10.09

Project Supervisor

Surname	Villari
Name	Massimo
Department	MIFT
Laboratory	fcrlab
E-mail	mvillari@unime.it
Phone number	

Project Co-Supervisor

Surname	
Name	
Job Position	
Department	

Laboratory	
E-mail	
Phone number	

Project details

Title	Cybersecurity and AI for Cloud, Edge, and Trusted Execution Environments (TEE)

Detailed description: 1. Objectives:

Develop skills in cloud and edge security, including confidential computing and TEEs.

Design and deploy AI workloads that preserve confidentiality and integrity in cloud and on-premise TEE environments.

Understand how to build trustworthy AI services (privacy, integrity, compliance, transparency) across cloud–edge pipelines.

2. Learning Outcomes
By the end, interns will be able to:

Explain and compare Rich Execution Environment (REE) vs Trusted Execution Environment (TEE), remote attestation, and secure execution.

Design a basic cloud–edge architecture where sensitive AI inference or feature extraction runs inside a TEE at the edge or on-prem, with encrypted channels to cloud backends.

Apply privacy and trust principles (encryption in transit/at rest/in use, minimal data exposure, auditability) to AI pipelines.

Document threats and mitigations for AI services (e.g., model theft, data leakage, prompt injection for LLM-based services).

Duration (month – max 12)	12
Duration (hours)	80
Open positions	4

Internship Skills

Technical requirements: CyberSecurity Course, Python language, Cloud and Edge Systems with their Virtualization and Big Data Management	
Other skills	Networking functionalities