Koffi Ismael Ouattara

PhD Candidate in AI Security — Ulm University & Huawei (Paris/Munich)
ouattaraismael1999@gmail.com — ouatt-isma.github.io — github.com/Ouatt-Isma — LinkedIn

Summary

PhD candidate in AI Security with hands-on experience in trustworthy machine learning, adversarial ML defenses, and applied R&D. Strong mix of academic output (6 papers, 1 patent) and industry projects (Huawei, Nokia Bell Labs, Mithril Security). Experienced with large-scale ML systems, trust modeling, and applied security.

Skills

Programming: Python, NodeJS, C++, C, Java, Rust, Go, R, x86_64 Assembly
Machine Learning: PyTorch, TensorFlow, Deep Learning, NLP, Transformers, Reinforcement Learning
Security/Networking: IDS/IPS (Snort, YARA), TCP/IP, DNS, DHCP, HTTP, adversarial ML
Tools: Docker, Git/GitHub, LaTeX
Languages: French (native), English (advanced), Chinese (basic), Spanish (basic)

Experience

Huawei Technologies & Ulm University — *PhD Student, AI Security* — Paris/Munich, 2023–Present

- Researched interpretable trust propagation in neural networks using Subjective Logic.
- Built the **Parallel Trust Assessment System (PTAS)**: dynamic trust scoring integrating data quality, model parameters, and inference context. Neuro symbolic for policy enforcement in AI Agent.
- Contributed to EU HORIZON projects (CONNECT, CASTOR, DUCA) designing trust frameworks for edge computing and secure AI.

Mithril Security — *Machine Learning / Security Engineer* — Paris, France, 2022–2023

- Developed defenses against model extraction and membership inference attacks.
- Enhanced robustness of deployed ML and LLM APIs in enterprise security contexts.

Nokia Bell Labs (Alcatel-Lucent Int.) — *Research Intern* — Nozay, France, 2022

- Designed ML-based anomaly detection for 5G networks with knowledge-graph convolutional networks.
- Co-inventor on US patent **US20240121678A1** (rogue base-station detection).

INRIA — *Research Intern* — Rennes, France, 2021
Designed meta-model of cryptographic architectures to verify compliance with best practices.

ISEP (Engineering School) — *Adjunct Lecturer* — Paris, France, 2022
Taught labs on Intrusion Detection Systems to graduate students.

Education

Ulm University — Germany
PhD in AI Security (ongoing), V2X Networks, Trust in ML — 2023–Present

Telecom Paris, Institut Polytechnique de Paris — France
Engineer & Master's in Cybersecurity, Machine Learning, Mobile Networks — 2021–2023

École Polytechnique — France
Engineer/Master's in Cybersecurity & Machine Learning — 2018–2022

Selected Projects

CONNECT (EU HORIZON) — Designed federated trust infrastructure for connected mobility using Subjective Logic.
Subjective Neural Networks (under review at ICLR 2026) — Bayesian framework combining Beta–Bernoulli Dropout and Subjective Logic for trust-aware and interpretable uncertainty estimation.

Publications & Patent

7 peer-reviewed papers (*FUSION '24/'25*, *ICICS '25*, *ECAI/ECML-PKDD Workshop '25*); 1 journal article under review.
1 Patent: *Distributed ML for rogue base-station detection* (US20240121678A1, 2024).