Koffi Ismael Ouattara

🎓 Ph.D. Candidate in AI Security   🏛 Ulm University & Huawei, Munich
✉ ouattaraismael1999@gmail.com   ⌂ Ouatt-Isma   💼 KI. Ouattara   🌐 Website

Ph.D. candidate in AI Security with deep expertise in trust assessment, subjective logic, and machine learning. Experienced in both academic research and applied industrial innovation.

Research Interests: Trust assessment in AI systems | Neural network interpretability | Security of machine learning | Subjective Logic | Federated trust infrastructures

Employment History

Jan 2023 – Present   **Ph.D. Student,** Huawei Technologies, Paris, France
Research Topic: Working on dynamic and Interpretable Trust Propagation in Neural Networks using Subjective Logic. Developing the Parallel Trust Assessment System (PTAS) to integrate dataset trustworthiness, model parameters, and inference context into real-time, property-specific trust scores.

Apr 2022 – Mar 2023   **Part-time Machine Learning/Security Engineer,** Mithril Security, Paris, France
Task: Developed defenses against model extraction and membership inference attacks on deep learning models.

Mar 2022 – Sep 2022   **Research Intern,** Nokia Bell Labs (Alcatel-Lucent International), Nozay, France
Task: Developed ML-based anomaly/attack detection for 5G networks using knowledge graph convolutional networks.
Resulted in a patent proposal considered essential for standardization.

Apr 2022   **Interim Teacher,** ISEP, Paris, France
Teaching Focus: Delivered labs on Intrusion Detection Systems.

Apr 2021 – Aug 2021   **Research Intern,** INRIA, Rennes, France
Task: Designed a meta-model of cryptographic architectures for compliance verification with best practices.

Education

2023 – Present   **Ph.D. Candidate, Ulm University** — Germany
Specialization: V2X Networks, Machine Learning, and Trust
Research Topic: *Trust Assessment in AI Systems*
Affiliation: Huawei Technologies, Munich
Supervisors: Prof. Frank Kargl and Prof. Theo Dimitrakos

2021 – 2023   **Engineer Degree, Telecom Paris**
Master's Degree (IP Paris), Institut Polytechnique de Paris — France
Specialization: Cybersecurity, Machine Learning, and Mobile Networks
Focus: Machine Learning, Communication, and Security

2018 – 2022   **Engineer/Master's Degree, École Polytechnique** — France
Specialization: Cybersecurity and Machine Learning
Notable Courses: Cryptography, Network Security, Deep Learning, Applied Mathematics, Markov Chains

2016 – 2018   **Preparatory Classes (MPSI), INP-HB** — Yamoussoukro, Ivory Coast
Intensive program for entry into Grandes Écoles (France)

Research Publications

Journal Articles

1. K. I. Ouattara *et al.*, "Ptas: Parallel trust assessment system for neural networks," *Submitted to IEEE Transactions on Neural Networks and Learning Systems*, 2025, Under review.

Conference Proceedings

1. K. I. Ouattara, A. Petrovska, A. Hermann, N. Trkulja, T. Dimitrakos, and F. Kargl, "On subjective logic trust discount for referral paths," in *2024 27th International Conference on Information Fusion (FUSION)*, Rank: B, 2024. 🔗 DOI: 10.23919/FUSION59988.2024.10706345.

2. S. Kriaa, A. Feki, S. Papillon, T. Chene, and I. Ouattara, "Detecting fake base stations using knowledge graphs and ml-based techniques," in *2023 IEEE Virtual Conference on Communications (VCC)*, Nov. 2023, pp. 37–42. 🔗 DOI: 10.1109/VCC60689.2023.10474891.

Accepted Conference Papers

1. K. I. Ouattara, I. Krontiris, T. Dimitrakos, and F. Kargl, *Assessing ai training dataset trustworthiness - a use case on bias*, Accepted at BIAS 2025 Workshop, ECML PKDD 2025; Rank: A.

2. N. Fotos, K. I. Ouattara, D. S. Karas, I. Krontiris, W. Meng, and T. Giannetsos, *Actions speak louder than words: Evidence-based trust level evaluation in multi-agent systems*, Rank: B, Acceptance rate: 26%, ICICS, 2025. 🔗 URL: https://www.icics2025.org/.

3. K. I. Ouattara, I. Krontiris, T. Dimitrakos, and F. Kargl, *Quantifying Calibration Error in Neural Networks through Evidence-Based Theory*, Accepted at Fusion 2025 ; Rank: B, 2025.

4. K. I. Ouattara, A. Petrovska, I. Krontiris, T. Dimitrakos, and F. Kargl, *An optimized framework for dspg synthesis and trust network analysis with subjective logic*, To appear ; Rank: B ; Acceptance Rate: 35%, 2025.

Patents

1. K. I. Ouattara, S. Papillon, A. Feki, and K. A. Pantelidou, "Distributed machine learning solution for rogue base station detection," Patent US20240121678A1, Filed Patent, 2024. 🔗 URL: https://patents.google.com/patent/US20240121678A1/en.

Work in Progress

1. K. I. Ouattara, *Subjective Neural Network*, Developing a neural network framework that integrates Subjective Logic for structured uncertainty modeling. Introduced a Subjective Binary Neural Network (SBNN) using binomial opinions over binary weights, and a novel mapping of continuous subjective opinions to Dirichlet Processes for nonparametric belief representation. Focused on enabling interpretable and trust-aware inference in both discrete and continuous domains.

Skills

Programming Languages	🔖 C, C++, Java, Python, Rust, R, Go, Assembly (x86_64)
Machine Learning	🔖 PyTorch, TensorFlow, Keras, Deep Learning, NLP, Reinforcement Learning, Transformers, LLM
Security and Networking	🔖 Snort, YARA, IDS/IPS Techniques, DHCP Spoofing, DNS Hijacking, TCP SYN Flood
Tools and Frameworks	🔖 Docker, Git/GitHub, Zotero, LaTeX
Network Protocols	🔖 IP, TCP/UDP, DNS, DHCP, HTTP
Operating Systems	🔖 Unix/Linux, Windows
Languages	🔖 French (native), English (advanced), Chinese (beginner), Spanish (beginner)

Research Projects

2022 – 2025 **CONNECT (EU HORIZON Project)**
Focus: Privacy-preserving federated trust infrastructure for connected mobility and edge computing
Role: Designed and implemented the Trust Assessment Framework (TAF) for evaluating the trustworthiness of edge services using dynamic, distributed reasoning with Subjective Logic.

2024 – Present **CASTOR (EU HORIZON Project)**
Focus: Continuous assessment for security, trustworthiness, and resilience of software
Role: Developed global/local Trust Assessment Frameworks for secure service routing. Integrated Subjective Logic into dynamic trust quantification and evidence modeling.

2023 – Present **DUCA (EU HORIZON Project)**
Focus: Digital user-centric architecture for privacy-preserving services
Role: Developed a dual-dimensional trust model combining Parallel Trust Assessment System (PTAS) with Homomorphic Encryption. Applied Subjective Logic to reason over trust in AI models.

2022 – 2024 **STRUNEE (Huawei Internal Project)**
Project: Trust Level Evaluation Engine (TLEE)
Role: Designed a modular engine for evaluating complex trust expressions over DAGs. Integrated trust operators (e.g., consensus, deduction, discounting) for distributed AI trust computation.

References

Available on Request