Ozgur Ural, Ph.D.

Curriculum Vitae, November 1, 2026

Leiden, Netherlands • drozgurural@gmail.com • +31 6 2903 0434

ozgurural.github.io • Google Scholar • ORCID 0000-0003-1329-4303 • linkedin.com/in/uralozgur

Machine learning researcher working on **trustworthy AI for mission-critical systems**: evidence of how a model was trained and who owns it, robustness against attackers, and predictable timing when a model runs inside a real-time loop. Ph.D. in Electrical Engineering and Computer Science, Embry-Riddle Aeronautical University (2025), with a machine-learning dissertation on Proof-of-Learning and model watermarking and three first-author articles in IEEE Access. More than twelve years of professional experience in industry and research, including production systems in cybersecurity, defense and flight simulation; currently at Avion Full Flight Simulators, leading the company's enterprise AI strategy.

RESEARCH INTERESTS

- Trustworthy and verifiable machine learning: Proof-of-Learning, model watermarking, model provenance and ownership verification
- Security of machine learning: spoofing attacks on training records, adversarial robustness
- Blockchain-enhanced machine learning
- Machine learning in real-time and safety-critical systems
- Natural language processing for cyber security

EDUCATION

Ph.D. in Electrical Engineering and Computer Science Aug 2021 – Aug 2025

Embry-Riddle Aeronautical University, Daytona Beach, Florida, USA

- Dissertation: Enhancing Proof-of-Learning Security Against Spoofing Attacks Using Model Watermarking.
- Advisor: Dr. Kenji Yoshigoe (Committee Chair); committee included IEEE Fellow Dr. Houbing Song.

M.Sc. in Cyber Security 2015 – 2019

Middle East Technical University (METU), Ankara, Turkey

- Thesis: Automatic Detection of Cyber Security Events from Turkish Twitter Stream and Turkish Newspaper Data.
- Advisor: Prof. Cengiz Acartürk.

B.Sc. in Computer Engineering 2010 – 2014

Middle East Technical University (METU), Ankara, Turkey

- English-medium programme; entered among roughly the top 1,000 of more than 2 million national candidates.

Bachelor of Business Administration 2012 – 2017

Anadolu University, Eskisehir, Turkey

PUBLICATIONS

Google Scholar (November 2026): 51 citations, h-index 4.

Journal Articles

[J3] **Ural, O.** and Yoshigoe, K. (2025). SecurePoL: Integration of Watermarking With Proof-of-Learning to Enhance Security Against Spoofing Attacks. *IEEE Access*, vol. 13, pp. 213067–213091. DOI: 10.1109/ACCESS.2025.3642198. *Research article.*

[J2] **Ural, O.** and Yoshigoe, K. (2024). Enhancing Security of Proof-of-Learning Against Spoofing Attacks Using Feature-Based Model Watermarking. *IEEE Access*, vol. 12, pp. 169567–169591. DOI: 10.1109/ACCESS.2024.3489776. *Research article.*

[J1] **Ural, O.** and Yoshigoe, K. (2023). Survey on Blockchain-Enhanced Machine Learning. *IEEE Access*, vol. 11, pp. 145331–145362. DOI: 10.1109/ACCESS.2023.3344669. *Survey article.*

IEEE Access: 2025 Journal Impact Factor 4.2 (JCR 2026).

Conference Papers

[C2] **Ural, O.** and Acartürk, C. (2021). Automatic Detection of Cyber Security Events from Turkish Twitter Stream and Newspaper Data. In *Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP 2021)*, pp. 66–76. DOI: 10.5220/0010201600660076.

[C1] Yamaç, A. Ö., Doçi, J., **Ural, O.**, Özarslan, Ö. F. and Temizer, S. (2014). Clover: Autonomous Cargo and Mail Delivery. *Turkish Autonomous Robots Conference (TORK 2014)*, Ankara, Turkey.

Theses

[T2] **Ural, O.** (2025). Enhancing Proof-of-Learning Security Against Spoofing Attacks Using Model Watermarking. Doctoral dissertation, Embry-Riddle Aeronautical University.

[T1] **Ural, O.** (2019). Automatic Detection of Cyber Security Events from Turkish Twitter Stream and Turkish Newspaper Data. Master's thesis, Middle East Technical University.

Technical Reports (not peer reviewed)

[R1] **Ural, O.** and Erdur, E. (2016). Secure Proxy on Cloud. Technical report. DOI: 10.13140/RG.2.2.24058.08649.

Narrated explainers of this research: ozgurural.github.io/lab.

RESEARCH EXPERIENCE

Graduate Research Assistant Sep 2021 – Dec 2024, May 2025 – Oct 2025

Embry-Riddle Aeronautical University, Daytona Beach, Florida, USA. Advisor: Dr. Kenji Yoshigoe

- Original research on verifiable, trustworthy machine learning across Proof-of-Learning, model watermarking and adversarial robustness, published as three first-author IEEE Access articles [J1–J3] and the doctoral dissertation [T2].

M.Sc. Thesis Research 2015 – 2019

Middle East Technical University, Ankara, Turkey. Advisor: Prof. Cengiz Acartürk

- Automatic detection of cyber security events from Turkish Twitter and newspaper data [T1], published at ICISSP 2021 [C2].

PROFESSIONAL SERVICE

- **Program Committee (2026):** NLPAICS 2026, 2nd Workshop on NLP Applied to Information and Cyber Security, Alicante.
- **Reviewer:** IEEE Access and other journals; IEEE and ACM conferences (security, machine learning, distributed systems).

AWARDS

- First Prize, TUBITAK national project competition (2014).
- Second Prize, METU Computer Engineering graduation Demo Day (2014).

INDUSTRY EXPERIENCE

Senior Software Engineer Oct 2023 – Present

Avion Full Flight Simulators, Nieuw-Vennep, Netherlands

- Lead Avion's enterprise AI strategy: authored the AI adoption roadmap and a three-tier architecture spanning air-gapped on-prem LLMs, a governed cloud-LLM API tier, and edge deployment.
- Designed the strategy's proposed AI workflows, each keeping a person accountable for the outcome; built engineering-knowledge retrieval prototypes and the strategy portal end to end.
- Developed real-time simulator software in C, C++ and Scala, including a low-latency telemetry pipeline sustaining approximately 50 GB/s with batching and bounded-queue backpressure.

Software Team Lead Nov 2020 – Aug 2021

Havelsan, Ankara, Turkey

- Led a team of 14 engineers (developers, QA, DevOps, support) delivering the Havelsan DLP endpoint Data Leakage Prevention product; developed core endpoint-agent features in C, C++, Java and Go.

Expert Software Engineer Feb 2019 – Nov 2020

STM Defence Technologies, Ankara, Turkey

- Developed mission-control and ground-control components for the Kargu and Togan autonomous UAVs in C++11 with Boost and Qt, under hard-real-time, safety-critical constraints; designed Power-On and Continuous Built-In Tests.

Expert Software Engineer Jul 2014 – Feb 2019

Comodo Cybersecurity, Ankara, Turkey

- Led design and development of Windows services and applications in C++17 with Boost and WinAPI (Comodo Dome Secure Web Gateway, Comodo Patch Manager, Comodo Dragon browser); established unit testing, code review and Jenkins CI/CD.

TECHNICAL SKILLS

- **Machine learning:** PyTorch, TensorFlow, scikit-learn, deep learning, LLMs, retrieval-augmented generation, federated learning; model watermarking, Proof-of-Learning, adversarial robustness
- **Languages:** C, C++, Scala, Python, Go, Java, TypeScript, JavaScript
- **Systems:** real-time and distributed systems, multithreading, low-latency pipelines, Linux, gRPC, Protobuf, Redis, PostgreSQL, Docker, GitLab CI/CD, Jenkins, Git