

Pedro Miguel Sánchez Sánchez

Senior Researcher — AI, Federated Learning, Cybersecurity & Secure Distributed Systems

✉ pedromiguelsanchezsanchez@gmail.com ☎ +34618235994 in pedromiguelsanchezsanchez 📧 sxz0

About Me

I hold a Ph.D. in Computer Science and am currently a Senior Researcher at Funditec. My doctoral research focused on enhancing IoT cybersecurity through applied Machine Learning and Deep Learning, specifically for device behavior fingerprinting and cyberattack detection, in collaboration with armasuisse S&T, Switzerland. Following my Ph.D., I shifted to research on Decentralized Federated Learning and AI Trustworthiness, applying these concepts to IoT cybersecurity, foundation models, and beyond. I keep myself updated by taking additional applied courses on topics such as Computer Vision, NLP, or AI agents.


Experience

- Senior Researcher**, *Funditec (Advantix Technology Foundation)* Madrid, Spain Nov 2024 – ...
 - Working on applied ML/DL and Cybersecurity
 - European and National research grant preparation, project execution, and administration
- Postdoctoral Researcher**, *University of Murcia* Murcia, Spain Feb 2024 – Nov 2024
 - New methods in Federated Learning and trustworthy AI assessment → armasuisse S&T collaboration
 - Contributed to EU-GUARDIAN EDF and ROBUST-6G Horizon projects
- Visiting Researcher**, *Cyber-Defence Campus, armasuisse S&T* Thun, Switzerland Sept–Dec 2021, 2022
 - Visiting researcher for six months (two three-month periods) in the context of my PhD thesis
- Predoctoral Researcher**, *University of Murcia* Murcia, Spain Sept 2019 – Feb 2024
 - Worked on IoT device behavior modeling for identification and attack detection, funded by armasuisse S&T





Education

- Ph.D. in Computer Science**, Cum Laude. *University of Murcia* Sept 2019 – Feb 2024
 - Thesis: *Identical IoT device identification via hardware performance fingerprinting and Machine Learning*
 - Supported by *armasuisse S&T*, also involved in the EU-GUARDIAN EDF and 5GZORRO H2020 projects
- M.Sc. in Computer Science**, 9.07/10. *University of Murcia* Sept 2018 – June 2019
 - Thesis: *Securing Smart Offices through an Intelligent and Multi-device Continuous Authentication System*
- B.Sc. in Computer Science**, 8.04/10. *University of Murcia* Sept 2014 – June 2018
 - Graduated with honors. Networking Specialization. Thesis: *Continuous authentication for mobile devices*


Research

16 h-index (+20 JCR journals, +10 confs, +4 chapters). Relevant research on Federated Learning, applied ML/DL in IoT behavior security, and AI Trustworthiness. Updated publication list in [Google Scholar](#) .

Relevant Projects (Grants and Code)

- [NEBULA](#)  Decentralized Federated Learning Platform → Research, design and implementation advice
- [EU-GUARDIAN EDF](#) , Cyber defence automation → Research, architecture design, and implementation
- [ROBUST-6G](#)  and [5G-ZORRO](#)  Horizon projects on distributed AI for networks → Research and design

Awards and Achievements

- National Young Researcher Award in Computer Science** 2024
 - Granted by the Scientific Society of Computer Science of Spain and the BBVA Foundation 
- Outstanding PhD Thesis Award** 2024
 - Award for the best Computer Science PhD Thesis in 2024 at my university (University of Murcia)
- Elsevier Computer Networks Best Paper Award** 2024
 - "Federated learning for malware detection in IoT devices", a collab with EPFL, UZH, and CYD Campus
- Conference Travel Grant and Volunteering** 2022, 2023
 - Student grants for conference attendance/volunteering: AAAI'23, ACM SIGCOMM'23, IEEE NOMS'22
- Secure and Private AI Scholarship Nanodegree** 2019
 - One of the 5000 recipients of 2019 Udacity's Secure and Private AI Scholarship sponsored by *Facebook*. Topics covered: Federated Learning, Differential Privacy, Homomorphic Encryption.

Technical Skills

Specialties: Federated Learning, AI Trustworthiness, Machine/Deep Learning, Cybersecurity, Behavior, IoT
Programming and Frameworks: Python, Bash, Keras, PyTorch, scikit-learn, C/C++, Java
Additional courses: HuggingFace AI Agents, HuggingFace Computer Vision, HuggingFace NLP

Annex. Main Publications

- [1] **Sánchez Sánchez, Pedro Miguel**, E. T. Martínez Beltrán, M. Fernández Llamas, G. Bovet, G. Martínez Pérez, and A. Huertas Celdrán, “Profe: Communication-efficient decentralized federated learning via distillation and prototypes,” in *Proceedings of the IEEE International Conference on Communications (IEEE ICC)*. IEEE, 2025, p. Accepted.
- [2] **Sánchez Sánchez, Pedro Miguel**, A. Huertas Celdrán, G. Bovet, and G. Martínez Pérez, “Transfer learning in pre-trained large language models for malware detection based on system calls,” in *MILCOM 2024-2024 IEEE Military Communications Conference (MILCOM)*. IEEE, 2024, pp. 853–858.
- [3] **Sánchez Sánchez, Pedro Miguel**, A. Huertas Celdrán, N. Xie, G. Bovet, G. Martínez Pérez, and B. Stiller, “Federatedtrust: A solution for trustworthy federated learning,” *Future Generation Computer Systems*, vol. 152, pp. 83–98, 2024.
- [4] **Sánchez Sánchez, Pedro Miguel**, A. Huertas Celdrán, G. Bovet, and G. Martínez Pérez, “Adversarial attacks and defenses on ml-and hardware-based iot device fingerprinting and identification,” *Future Generation Computer Systems*, vol. 152, pp. 30–42, 2024.
- [5] A. Huertas Celdrán, **Sánchez Sánchez, Pedro Miguel**, J. Von Der Assen, T. Schenk, G. Bovet, G. Martínez Pérez, and B. Stiller, “Rl and fingerprinting to select moving target defense mechanisms for zero-day attacks in iot,” *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 5520–5529, 2024.
- [6] C. Feng, A. Huertas Celdrán, J. Baltensperger, E. T. Martínez Beltrán, **Sánchez Sánchez, Pedro Miguel**, G. Bovet, and B. Stiller, “Sentinel: An aggregation function to secure decentralized federated learning,” in *European Conference on Artificial Intelligence (ECAI) 2024*. IOS Press, 2024, pp. 1760–1767.
- [7] **Sánchez Sánchez, Pedro Miguel**, A. Huertas Celdrán, G. Bovet, and G. Martínez Pérez, “Single-board device individual authentication based on hardware performance and autoencoder transformer models,” *Computers & Security*, vol. 137, p. 103596, 2024.
- [8] **Sánchez Sánchez, Pedro Miguel**, A. Huertas Celdrán, T. Schenk, A. L. B. Iten, G. Bovet, G. Martínez Pérez, and B. Stiller, “Studying the robustness of anti-adversarial federated learning models detecting cyberattacks in iot spectrum sensors,” *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 2, pp. 573–584, 2024.
- [9] E. T. Martínez Beltrán, **Sánchez Sánchez, Pedro Miguel**, S. López Bernal, G. Bovet, M. Pérez Gil, G. Martínez Pérez, and A. Huertas Celdrán, “Fedstellar: A platform for training models in a privacy-preserving and decentralized fashion,” in *International Joint Conference on Artificial Intelligence (IJCAI-23) Demos*, 2023.
- [10] A. Huertas Celdrán, J. Kreischer, M. Demirci, J. Leupp, **Sánchez Sánchez, Pedro Miguel**, M. Franco Figueredo, G. Bovet, G. Martínez Pérez, and B. Stiller, “A framework quantifying trustworthiness of supervised machine and deep learning models,” in *SafeAI2023: The AAAI’s Workshop on Artificial Intelligence Safety*, 2023, pp. 2938–2948.
- [11] E. T. Martínez Beltrán, M. Pérez Quiles, **Sánchez Sánchez, Pedro Miguel**, S. López Bernal, G. Bovet, M. Pérez Gil, G. Martínez Pérez, and A. Huertas Celdrán, “Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges,” *IEEE Communications Surveys & Tutorials*, vol. 25, no. 4, p. 2983–3013, 2023.
- [12] V. Rey, **Sánchez Sánchez, Pedro Miguel**, A. Huertas Celdrán, and G. Bovet, “Federated learning for malware detection in iot devices,” *Computer Networks*, vol. 204, p. 108693, 2022.
- [13] **Sánchez Sánchez, Pedro Miguel**, J. M. Jorquera Valero, A. Huertas Celdrán, G. Bovet, M. Pérez Gil, and G. Martínez Pérez, “A survey on device behavior fingerprinting: Data sources, techniques, application scenarios, and datasets,” *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1048–1077, 2021.