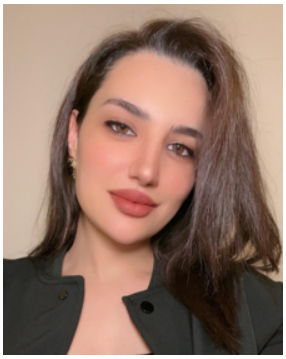
Dr.-Ing. Engr. Amira Guesmi

Research Group Leader at Electrical and Computer Engineering

New York University Abu Dhabi (NYUAD), UAE



Email: guesmiamira1@gmail.com, ag9321@nyu.edu

Language Skills: English (Fluent), French (Fluent), Arabic (Native).

Google Scholar: https://scholar.google.com/citations?user=ramnnXoAAAAJ&hl=en&oi=sra
[Total Citations: 150+; h-index: 8; i10-index: 5]

DBLP: https://dblp.org/pid/247/5179.html

Job Experience: Extensive experience in developing secure frameworks and techniques to protect machine learning models and data from adversarial and backdoor attacks, identifying vulnerabilities in AI systems. Created methods to ensure the privacy of data in machine learning processes. Investigated approaches to make deep learning models more interpretable, enhancing transparency and trust in their decisions and predictions. Explored cutting-edge techniques in computer vision, and designed and optimized computing systems to achieve high performance with minimal energy consumption. Managed and collaborated on multiple projects simultaneously and contributed open-source projects, fostering community engagement and innovation.

Personality: Goal-oriented, Team player, Creative and Innovative, Out-of-the-Box Thinker, Ambitious, Committed, Facing new challenges, Quick learner, Self-critical, Excellent communication and organizational skills.

Education

Oct. 2018 – Oct. 2021 **Ph.D. in Computer Engineering *(Summa cum laude)***
Department of Computer Science & Electrical Engineering, University of Sfax (US) - National Engineering School of Sfax (ENIS), Tunisia
IEMN-DOAE, Polytechnic University Hauts-De-France (UPHF), France
Thesis: "A Study of Deep Neural Networks Performance and Robustness under Adversarial Attacks"

Sep. 2012 – Sep. 2016 **Eng. Computer Science & Electrical Engineering *(Magna cum laude)***
Department of Computer Science & Electrical Engineering, University of Sfax (US) - National Engineering School of Sfax (ENIS), Tunisia

Sep. 2010 – Jun. 2012 **Preparatory Cycles to Engineering Studies**
El Manar Preparatory Engineering Institute (IPEIEM), Tunis, Tunisia

Professional Experience

Sep. 2022 – To Date **Research Group Leader**, Department of Electrical and Computer Engineering, Division of Engineering, New York University – Abu Dhabi (NYUAD), UAE.

Dec. 2021 – Aug. 2022 **Postdoctoral Associate**, IEMN-DOAE, Polytechnic University Hauts-De-France (UPHF), Valencienne, France.

Jun. 2018 – Sep. 2018 **Research Assistant**, Professur für Mess-und Sensortechnik, Chemnitz University of Technology, Chemnitz, Germany.

Sep. 2017 – May. 2018 **Research Assistant**, Department of Computer Science & Electrical Engineering, National Engineering School of Sfax (ENIS), Sfax, Tunisia.

Sep. 2016 – Aug. 2017 **Research Assistant**, Department of Mathematics, Statistics and Computer Science, Marquette University, Wisconsin, USA.

Jan. 2016 – Jun. 2016 **Research and Development Intern**, Professur für Mess-und Sensortechnik, Chemnitz University of Technology, Chemnitz, Germany.

Summary of Key Research Output

Publications 1 Book, 10+ Scientific Publications, ~20 Archive Papers.
(in top-tier Conferences like CVPR, ASPLOS, IROS, DAC, etc, and in top-tier IEEE Journals like D&T, Access, etc.)

Awards and Recognitions Awarded Best Senior Researcher, eBRAIN Lab, NYUAD, 2023.

Grant Recipient *"Advanced Technologies based on Internet of Things (ATIoT)"* funded by DAAD (Deutscher Akademischer Austausch Dienst), *2018*

Grant Recipient *"Promotion of young talents in embedded systems for energy management (Young ESEM)"* within the program: *"Deutsch-Arabische Hochschulpartnerschaften",* 2016.

Student Co-advising 2 PhD Students, 10+ Interns & BS/MS Theses co- supervised

Research Interests

- Secure Machine Learning
- Adversarial and Backdoor Attacks
- Privacy-Preserving ML
- Continual Learning
- DL Models Interpretability
- Computer Vision
- Approximate Computing
- Low-Power Design
- Energy-Efficient Computing

Grants and Research Projects

Research Proposals and Third-Party Funding [Accepted and Submitted Proposals]

CASTLE: Cross-Layer Security for Machine Learning Systems in IoT (Accepted)

3.5-years [2022 – 2025] Project Proposal funded by the Technology Innovation Institute (TII) under Advanced Technology Research Council (ATRC), Abu Dhabi, UAE
Total Grant: $1.855 Million (AED 6.81 Million)
Role: Research and Concept Development (R&D)
PI: Muhammad Shafique

RESIST: Robustness and Ethics of Intelligent Surveillance Systems (Accepted)

1-year [2021 – 2022] Project Proposal funded by Region Hauts-de-France and the partners are: Luxant Innovation, Université Polytechnique Hauts-de-France and Université de Lille, France.
Total Grant: 40K USD.
Role: Research and Concept Development (R&D)
PI: Ihsen Alouani

List of Publications

Journals / Transactions Publications (Accepted / Published)

[J1] **A. Guesmi,** M. A. Hanif, B. Ouni, M. Shafique, "SAAM: Stealthy Adversarial Attack on Monocular Depth Estimation", in **IEEE Access**, vol. 12, pp. 13571-13585, doi: 10.1109/ACCESS.2024.3353042, 2024

[J2] **A. Guesmi**, M. A. Hanif, B. Ouni and M. Shafique, "Physical Adversarial Attacks for Camera-Based Smart Systems: Current Trends, Categorization, Applications, Research Challenges, and Future Outlook", in **IEEE Access**, vol. 11, pp. 109617-109668, 2023.

[J3] **A. Guesmi,** M. A. Hanif and M. Shafique, "AdvRain: Adversarial Raindrops to Attack Camera-Based Smart Vision Systems. Information", in **Information** 14, no. 12: 634, 2023.

[J4] **A. Guesmi**, I. Alouani, M. Baklouti, T. Frikha and M. Abid, "SIT: Stochastic Input Transformation to Defend Against Adversarial Attacks on Deep Neural Networks", in **IEEE Design & Test**, vol. 39, no. 3, pp. 63-72, 2022.

Peer-Reviewed Conference/Symposium Publications: Accepted / Published

[C1] **A. Guesmi**, R. Ding, M. A. Hanif, I. Alouani and M. Shafique, "DAP: A Dynamic Adversarial Patch for Evading Person Detectors", The IEEE / CVF Computer Vision and Pattern Recognition Conference (**CVPR**) 2024. (Accepted)

[C2] **A. Guesmi**, M. A. Hanif, I. Alouani, B. Ouni, M. Shafique, "SSAP: A Shape-Sensitive Adversarial Patch for Comprehensive Disruption of Monocular Depth Estimation in Autonomous Navigation Applications", IEEE/RSJ International Conference on Intelligent Robots and Systems (**IROS)** 2024. (Accepted)

[C3] N. Chattopadhyay, **A. Guesmi**, M. A. Hanif, B. Ouni, and M. Shafique, "DefensiveDR: Defending against Adversarial Patches using Dimensionality Reduction", The ACM/IEEE Design Automation Conference (**DAC**) 2024. (Accepted)

[C4] **A. Guesmi**, N. S. Aswani, M. Shafique, "Exploring the Interplay of Interpretability and Robustness in Deep Neural Networks: A Saliency-guided Approach", Security and Privacy of Machine Learning-based Vision Processing in Autonomous Systems (**SPVis**), 2024. (Accepted)

[C5] N. S. Aswani, **A. Guesmi**, M. Shafique, "Examining Changes in Internal Representations of Continual Learning Models Through Tensor Decomposition", ContinualAI **The Unconference**, 2024. (Accepted)

[C6] **A. Guesmi**, I. M. Bilasco, M. Shafique, I. Alouani, "AdvART: Adversarial Art for Camouflaged Object Detection Attacks", IEEE International Conference on Image Processing (**ICIP**) 2024. (Accepted)

[C7] N. Chattopadhyay, **A. Guesmi**, M. Shafique, "Anomaly Unveiled: Securing Image Classification against Adversarial Patch Attacks", IEEE International Conference on Image Processing (**ICIP**) 2024. (Accepted)

[C8] A. Arous, **A. Guesmi**, M. A. Hanif, I. Alouani and M. Shafique, "Exploring Machine Learning Privacy/Utility Trade-Off from a Hyperparameters Lens", International Joint Conference on Neural Networks (**IJCNN**), 1-10, 2023.

[C9] **A. Guesmi**, K. N. Khasawneh, N. Abu-Ghazaleh and I. Alouani, "ROOM: Adversarial Machine Learning Attacks Under Real-Time Constraints", International Joint Conference on Neural Networks (**IJCNN**), pp. 1-10, 2022.

[C10] S. Dave, A. Marchisio, M.A. Hanif, **A. Guesmi,** A. Shrivastava, I. Alouani, M. Shafique, "Special session: Towards an agile design methodology for efficient, reliable, and secure ML systems", In IEEE 40th VLSI Test Symposium (**VTS**) (pp. 1-14). IEEE, 2022.

[C11] **A. Guesmi,** I. Alouani, K. N. Khasawneh, M. Baklouti, T. Frikha, M. Abid and N. Abu-Ghazaleh, "Defensive approximation: securing CNNs using approximate computing", The ACM international conference on architectural support for programming languages and operating systems (**ASPLOS**), 2021.

[C12] **A. Guesmi,** I. Alouani, M. Baklouti, T. Frikha, M. Abid, and A. Rivenq, "HEAP: A Heterogeneous Approximate Floating-Point Multiplier for Error Tolerant Applications", In Proceedings of the 30th International Workshop on Rapid System Prototyping (**RSP**), 2019.

[C13] D. El Houssaini, **A. Guesmi**, S. Khriji, T. Keutel, K. Besbes, O. Kanoun, "Experimental investigation on weather changes influences on wireless localization system", In IEEE International Symposium on Measurements & Networking (**M&N**) (pp. 1-6). IEEE, 2019.

Archive Articles

[A1] **A. Guesmi**, N. S. Aswani, M. Shafique, "Exploring the Interplay of Interpretability and Robustness in Deep Neural Networks: A Saliency-guided Approach", CoRR abs/2405.06278, 2024.

[A2] N. S. Aswani, **A. Guesmi**, M. Shafique, "Examining Changes in Internal Representations of Continual Learning Models Through Tensor Decomposition", CoRR abs/2405.03244, 2024.

[A3] **A. Guesmi**, M. A. Hanif, I. Alouani, B. Ouni, M. Shafique, "SSAP: A Shape-Sensitive Adversarial Patch for Comprehensive Disruption of Monocular Depth Estimation in Autonomous Navigation Applications", CoRR abs/2403.11515, 2024.

[A4] **A. Guesmi**, I. M. Bilasco, M. Shafique, I. Alouani, "AdvART: Adversarial Art for Camouflaged Object Detection Attacks", CoRR abs/2303.01734, 2023.

[A5] N. Chattopadhyay, **A. Guesmi**, M. Shafique, "Anomaly Unveiled: Securing Image Classification against Adversarial Patch Attacks", CoRR abs/2402.06249, 2023.

[A6] **A. Guesmi**, M. A. Hanif, B. Ouni, M. Shafique, "SAAM: Stealthy Adversarial Attack on Monocular Depth Estimation", CoRR abs/2308.03108, 2023.

[A7] N. Chattopadhyay, **A. Guesmi**, M. A. Hanif, B. Ouni, M. Shafique, "DefensiveDR: Defending against Adversarial Patches using Dimensionality Reduction", CoRR abs/2311.12211, 2023.

[A8] **A. Guesmi**, M. A. Hanif, I. Alouani, M. Shafique, "APARATE: Adaptive Adversarial Patch for CNN-based Monocular Depth Estimation for Autonomous Navigation", CoRR abs/2303.01351, 2023.

[A9] **A. Guesmi**, R. Ding, M. A. Hanif, I. Alouani, M. Shafique, "DAP: A Dynamic Adversarial Patch for Evading Person Detectors", CoRR abs/2305.11618, 2023.

[A10] N. Chattopadhyay, **A. Guesmi**, M. A. Hanif, B. Ouni, M. Shafique, "ODDR: Outlier Detection & Dimension Reduction Based Defense Against Adversarial Patches", CoRR abs/2311.12084, 2023.

[A11] **A. Guesmi**, M. A. Hanif, M. Shafique, "AdvRain: Adversarial Raindrops to Attack Camera-based Smart Vision Systems", CoRR abs/2303.01338, 2023.

[A12] A. A. Hamza, **A. Guesmi**, I. Dayoub, I. Alouani, "AaN: Anti-adversarial Noise - A Novel Approach for Securing Machine Learning-based Wireless Communication Systems", TechRxiv. October 12, 2023. DOI: 10.36227/techrxiv.24268543.v1

[A13] **A. Guesmi**, M. A. Hanif, B. Ouni, M. Shafique, "Physical Adversarial Attacks For Camera-based Smart Systems: Current Trends, Categorization, Applications, Research Challenges, and Future Outlook", CoRR abs/2308.06173, 2023

[A14] A. Arous, **A. Guesmi**, M. A. Hanif, I. Alouani, M. Shafique, "Exploring Machine Learning Privacy/Utility trade-off from a hyperparameters Lens", CoRR abs/2303.01819, 2023.

[A15] S. Dave, A. Marchisio, M.A. Hanif, **A. Guesmi**, A. Shrivastava, I. Alouani, M. Shafique, "Special session: Towards an agile design methodology for efficient, reliable, and secure ML systems", CoRR abs/2204.09514, 2022.

[A16] **A. Guesmi,** I. Alouani, "Adversarial Attack on Radar-based Environment Perception Systems", CoRR abs/2211.01112, 2022.

[A17] **A. Guesmi,** I. Alouani, K. N. Khasawneh, M. Baklouti, T. Frikha, M. Abid and N. Abu-Ghazaleh, "Defending with Errors: Approximate Computing for Robustness of Deep Neural Networks", CoRR abs/2211.01182, 2022.

[A18] **A. Guesmi,** K. N. Khasawneh, N. Abu-Ghazaleh, I. Alouani, "ROOM: Adversarial Machine Learning Attacks Under Real-Time Constraints", CoRR abs/2201.01621, 2022.

[A19] **A. Guesmi,** I. Alouani, K. N. Khasawneh, M. Baklouti, T. Frikha, M. Abid and N. Abu-Ghazaleh, "Defensive approximation: securing CNNs using approximate computing", CoRR abs/2006.07700, 2020.

Co-advising/Supervision of PhD Students, MS/BS Thesis Students, and Interns

PhD Students/Researchers under my Co-advising

1. **Nishant Aswani [2021 – 2026]:** Embedded Lifelong Learning for Coordinated Autonomous Systems
2. **Soukaina Aji [2022]:** Security and Privacy of Neuromorphic Computing Systems

MS/BS Theses Students

1. **Taha Yassine Abidi** [Spring 2022 - Summer 2022]
2. **Ayoub Arous** [Spring 2022 - Summer 2022]

Student Research Assistants

1. **Basil Ahmed** [Fall 2022 – Spring 2024]
2. **Hashim Zia** [Fall 2022 – Spring 2024]
3. **Shahram Chaudhry** [Fall 2022 – Spring 2024]
4. **Abdullah Suri** [Fall 2022 – Spring 2024]
5. **Victor Ruitian Ding** [Fall 2022 – Spring 2023]
6. **Aavishkar Gautam** [Fall 2022 – Spring 2023]
7. **Adam Sharif** [Fall 2022 – Spring 2023]
8. **Prakrati Mamtani** [Spring 2024 – Fall 2024]
9. **Nikita Gupta** [Spring 2024 – Fall 2024]