Salah GHAMIZI

Postdoctoral Researcher @ Snt-University of Luxembourg

Tel: +33781780464 E-mail: salah.ghamizi@uni.lu
https://scholar.google.com/citations?user=UcvKgR0AAAAJ

Education

SnT - University of Luxembourg 2019-2022
Ph.D. Researcher: Robust Machine Learning for Critical Applications

Postdoctoral Researcher : Robust Machine Learning for Critical Applications 2022-2024

Selected papers:

- Dyrmishi, Salijona & Ghamizi, Salah & al. **How do humans perceive adversarial text? ; ACL23.**
- Ghamizi, Salah & Zhang, Jingfeng & al. **GAT: Data-efficient Adversarial Training with Self-supervised Auxiliary Tasks; ICML23;**
- Ghamizi, Salah & al. **On Evaluating Adversarial Robustness of Chest X-ray Classification: Pitfalls and Best Practices; accepted at AAAI23-SafeAI.**
- Dyrmishi, Salijona & Ghamizi, Salah & al. **On The Empirical Effectiveness of Unrealistic Adversarial Hardening Against Realistic Adversarial Attacks; accepted at S&P23.**
- Simonetto, Thibault & Ghamizi, Salah & al. **A Unified Framework for Adversarial Attack and Defense in Constrained Feature Space; IJCAI22.**
- Ghamizi, Salah & al. **Adversarial robustness in multi-task learning: Promises and illusions; AAAI22**
- Ghamizi, Salah & al. **Evasion Attack STeganography: Turning Vulnerability Of Machine Learning To Adversarial Attacks Into A Real-world Application; ICCV21-AROW;**
- Ghamizi, Salah & Renaud Rwemalika & al. **Data-driven Simulation and Optimization for Covid-19 Exit Strategies. *KDD 2020;* Best Paper**

Projects:

- STELLAR (2020-2023): Measuring and improving the quality of the ML systems and building safe and robust systems.
- PILOT (2020-2021): Supporing policymakers with simulation and forecasting tools of the COVID19 pandemic under noisy and scarce data/
- SVALINN (2023-2024): Protecting digital assets from various misuses including secret disclosure, tampering, and fake content generation.

Teaching duties:

- Applied Machine Learning (MADS-22) - Master 2022/2023
- Introduction to Machine Learning (ISM-22) - Master 2022/2023
- TA- Software Engineering (F1_BAINFOR-44) - Bachelor 2021/2022
- TA- Software Testing (BPINFOR-35) - Bachelor 2020/2021

Professional Service:

- Software Engineering Conference/Journal reviewer: ICSE20/21/22, FSE21/22/23, ISSTA21/22, SBSE22, TSE, TOSEM, EMSE
- ML/CV Conference/Journal reviewer: ECCV22, NeurIPS22, CVPR23, ICCV23
- Organization team: ICSME2020, SIMLA2023

GeorgiaTech / IAE Metz (France); 2016-2017

I-Corps/ Msc Entrepreneurship & Management of Innovative Businesses
Relevant Coursework: *Agile & Lean Projects, Team Management, Funding Proposal writing.*

MinesNancy, School of Computer Science 2012-2016
Bachelor then Master in Artificial Intelligence and Robotics.
Relevant Coursework: Algorithms, Data Structure, Artificial Intelligence, Image Analysis, Computer Architecture, Distributed Systems, Databases, Mobile & Web development, Probability & Statistics, Operations Research.
Capstone projects:

- ReTypograph; Using OpenCV-JAVA, text extraction & automated generation of text fonts from raw pictures of historical records (2014).
- iCrisis; tracking & prediction of crowd behavior in emergencies using video analysis with Optical Flows, wearable motion sensors, and RNN algorithms (2016).

Work Experience

BGL BNP Paribas, Sept 2019 Mars 2020
Research Scientist (intern)
As part of my PhD, I worked on the robustness of financial systems (Credit Scoring, Fraud detection) to adversarial attacks. Demonstrated the vulnerability of production systems to constrained attacks and designed a new MLOps pipeline to robustify and protect the system.

LumApps SAS, March 2018 Dec 2018
R&D Engineer
In charge of the improvements and deployment process of the platform of some of the company's major clients (Decathlon, Veolia,…) and implemented third party API integration: Set up the open-source SDK of the company, and supervised the continuous delivery & testing architecture of the SDK (React/Typescript ; Python).

WAZA Education, Sept 2016 March 2018
Co-founder and CTO
Fullstack lead engineer of a team of 3 people:
Built the MVP & Production platform using Angular & LAMP stack. Migrated the application to a GCloud scalable architecture with continuous deployment with Bitbucket pipelines. Sped up common user interaction up to 800% by refactoring runtime complexities & implementing caching and one-way bindings.

Recent Awards & Volunteering

Grants and awards:
FNR Jump (2023) - 250k€ from *Luxembourg National Research Fund for project SVALINN - Research on Adversarial Attacks applications in the real world (2 years)*
Excellent Thesis Award (2023) - *Highest distinction of PhD graduates in Luxembourg*
COVID-19 Task Force (2020) - 120k€ from *Luxembourg National Research Fund and AUF, research on robust forecasting on Covid19 pandemic with scarce and OOD data (1 year)*
EcoRevolutions, i-LAB (2016) - Awarded 12k€ from the *French Ministry of Research & Innovation* for project WAZA - Design of Recommender Systems for Edtech and Adaptive Learning
Imagine Cup (2016) – Finalist of the competition held by Microsoft France for project WAZA

Volunteering: JCI - Junior Chamber International (Vice President), TEDx MinesNancy (Founder).

Languages

French | Arabic
Mother tongues

English
Fluent, C1 level: Cambridge Advanced Examination