Aayush Garg

Nationality: Luxembourgish (EU citizen)
Email: aayushgarg.bu@gmail.com
Website: `https://draayushgarg.github.io`
GitHub: `https://github.com/garghub`
Google Scholar: `https://scholar.google.com/citations?user=UBOhgRAAAAAJ`

Research Interests

AI for Cybersecurity, Cyber Defense, Vulnerability Analysis and Prediction, Mutation Testing, Software Quality Assurance, Machine Learning, Large Language Models, Developer Experience

Education

Ph.D. in Computer Science   University of Luxembourg, Luxembourg
July 2019 – May 2023
Dissertation: *Guiding Quality Assurance Through Context Aware Learning*
Advisor: Prof. Yves Le Traon; Co-advisor: Prof. Mike Papadakis

M.S. in Computer Science   Boston University, USA
Concentration: *Security*
August 2017 – January 2019
GPA: 3.8/4.0

B.Tech. in Computer Science   Amity University, India
April 2006 – March 2010
GPA: 7.0/10.0

Research Experience

Postdoctoral Researcher   Luxembourg Institute of Science and Technology (LIST)
March 2024 – Present   Luxembourg

- Developing AI methods to improve software security, focusing on real and artificial vulnerabilities.
- Exploring Large Language Models (LLMs) for automated patch generation, software self-healing, and improved developer experience through code-assistance tools.
- Designing frameworks to transform threat intelligence into executable cyber range scenarios for training.
- Developing automated solutions to identify attack vectors in 5G-core networks.
- Utilizing Deep Learning, particularly Transformer architectures, to identify API fuzzing attack patterns.

Doctoral Researcher   Interdisciplinary Centre for Security, Reliability and Trust (SnT)
July 2019 – March 2024   University of Luxembourg

- Designed AI-driven solutions to automate feature extraction from source code, replacing manual efforts.
- Trained Neural Networks achieving up to 87% Precision and Recall in task-specific classifications.
- Employed LLMs and GPTs to induce artificial faults, increasing test effectiveness by up to 65%.

Teaching Experience

Teaching Assistant   Faculty of Science, Technology and Medicine (FSTM)
July 2019 – May 2023   University of Luxembourg

- Conducted lectures on "Introduction to Machine and Deep Learning" for Bachelors in Computer Science (BICS), mentoring students in AI-driven software development.
- Delivered lectures on "Introduction to Software Testing" for Bachelors in Applied Information Technology (BINFO), guiding students in secure coding methodologies.
- Recorded lecture series available online to support students during the COVID-19 lockdown.

Software Engineering Experience

Senior Software Engineer   Futures First, India
September 2014 – February 2017

- Developed multi-threaded Windows applications to process and display stock prices and trade updates with a 3-second refresh rate.
- Implemented microservices to capture up to 12 real-time stock price updates per second via market APIs.
- Engineered a Futures and Commodities trading platform, enabling a minimum of 95% of organizational market investments.

Senior Software Engineer   Indus Valley Partners, USA
August 2012 – September 2014

- Built investment-compliance applications to automate legal due diligence auditing, reducing manual effort by up to 85%.
- Implemented microservices to enable configurable email alerts, streamlining at least 80% of business process workflows.
- Integrated portfolio dashboards and reporting capabilities for 11 Business Experts (SMEs), facilitating comprehensive debt investment overviews.

Associate Software Engineer   Fiserv, USA
May 2010 – August 2012

- Crafted web applications to streamline investment portfolio metrics capturing, resulting in a 53% increase in efficiency.
- Resolved defects and maintained source code for three large-scale Electronic Fund Transfer banking projects.
- Ensured high-quality (minimum 85% defect-free) applications through peer-reviewing code modifications.

Causal Analysis and Resolution Coordinator   Fiserv, USA
May 2010 – August 2012

- Performed defect root cause analysis and processed inefficiencies for 95% of Business Unit projects.
- Executed corrective actions to drive continuous process enhancements, maintaining at least 85% defect-free software quality and achieving a 15% increase in module delivery efficiency per quarter.

Skills

- **Programming Languages:** Python, Java, C++, C#
- **AI/ML Frameworks & Libraries:** PyTorch, Pandas, TensorFlow, Keras, Scikit-learn, Hugging Face
- **Techniques:** Machine Learning, Deep Learning, Natural Language Processing, Prompt Engineering, Static and Dynamic Analysis
- **Security and Testing:** Vulnerability Assessment and Prediction, Artificial Vulnerability Generation, Vulnerability Injection, Mutation Testing
- **NLP and LLMs:** Large Language Models (LLM), Generative Pretrained Transformers (GPT), Neural Machine Translation (NMT), Encoder-Decoders, Transformers
- **Tools and Platforms:** Git, Docker, SQL Server, Apache Cassandra, RabbitMQ

Professional Activities

Conference and Workshop Roles

- **Track Chair:**
  - 29th International Conference on Evaluation and Assessment in Software Engineering (EASE 2025), Learnings/Reflections of Evaluation and Assessment Projects in Software Engineering (Learnings & Reflections) Track.
- **Program Committee Member:**
  - 40th IEEE/ACM International Conference on Automated Software Engineering (ASE 2025), New Ideas and Emerging Results (NIER) Track.
  - 34th International Symposium on Software Testing and Analysis (ISSTA 2025), Tool Demonstrations Track.
  - 39th IEEE/ACM International Conference on Automated Software Engineering (ASE 2024), NIER Track.
  - 17th IEEE International Conference on Software Testing, Verification and Validation (ICST 2024), Mutation 2024 Workshop.

Peer Reviewing (Journals)

- ACM Transactions on Software Engineering and Methodology (TOSEM) Journal, since November 2024.
- Springer International Journal of Machine Learning and Cybernetics, since October 2024.
- Springer Automated Software Engineering Journal, since September 2024.
- Springer International Journal of Information Security, since September 2024.
- Springer Scientific Reports, since May 2024.
- Elsevier Computers & Security Journal, since January 2024.
- Springer Software Quality Journal, since December 2023.
- Software Testing, Verification and Reliability (STVR) Journal, since December 2023.
- IEEE Transactions on Software Engineering (TSE) Journal, since August 2022.

Invited Talks and Presentations

- **ICST 2024**, Toronto, Canada: Presented "On the Coupling between Vulnerabilities and LLM-generated Mutants: A Study on Vul4J dataset," May 30, 2024.
- **ISSRE 2023**, Florence, Italy: Presented "Enabling Efficient Assertion Inference," October 12, 2023.
- **CREST, University of Adelaide**, Australia: Delivered guest lectures on "Guiding Quality Assurance Through Context Aware Learning," August 2023.

- **ICSE 2023**, Melbourne, Australia: Presented "Learning from What We Know: How to Perform Vulnerability Prediction using Noisy Historical Data," May 19, 2023.
- **ASE 2022**, Michigan, USA: Presented "Cerebro: Static Subsuming Mutant Selection," October 12, 2022.

Publications

1. **Aayush Garg**, Renzo Degiovanni, Mike Papadakis, Yves Le Traon. "On the Coupling between Vulnerabilities and LLM-generated Mutants: A Study on Vul4J dataset." *IEEE International Conference on Software Testing, Verification and Validation (ICST)*, 2024.

2. **Aayush Garg**, Yuejun Guo, Qiang Tang. "AI-Driven Software Security: Vulnerability Detection, Patching, and Anti-Fuzzing." *ERCIM News*, 2024.

3. **Aayush Garg**, Renzo Degiovanni, Facundo Molina, Mike Papadakis, Nazareno Aguirre, Maxime Cordy, Yves Le Traon. "Enabling Efficient Assertion Inference." *IEEE International Symposium on Software Reliability Engineering (ISSRE)*, 2023.

4. Milos Ojdanic, Ahmed Khanfir, **Aayush Garg**, Renzo Degiovanni, Mike Papadakis, Yves Le Traon. "On Comparing Mutation Testing Tools through Learning-based Mutant Selection." *ACM/IEEE International Conference on Automation of Software Test (AST)*, 2023.

5. **Aayush Garg**. "Guiding Quality Assurance Through Context Aware Learning." *Ph.D. Dissertation, University of Luxembourg Open Repository and Bibliography (ORBilu)*, 2023.

6. Milos Ojdanic, **Aayush Garg**, Ahmed Khanfir, Renzo Degiovanni, Mike Papadakis, Yves Le Traon. "Syntactic Vs. Semantic similarity of Artificial and Real Faults in Mutation Testing Studies." *IEEE Transactions on Software Engineering (TSE)*, 2023.

7. **Aayush Garg**, Renzo Degiovanni, Matthieu Jimenez, Maxime Cordy, Mike Papadakis, Yves Le Traon. "Learning from What We Know: How to Perform Vulnerability Prediction using Noisy Historical Data." *Empirical Software Engineering (EMSE)*, 2022.

8. **Aayush Garg**, Milos Ojdanic, Renzo Degiovanni, Thierry Titcheu Chekam, Mike Papadakis, Yves Le Traon. "Cerebro: Static Subsuming Mutant Selection." *IEEE Transactions on Software Engineering (TSE)*, 2021.

Papers Under Review

1. Anonymous authors, Title changed. "Benchmarking Large Language Models for Patching Artificial Software Vulnerabilities." Under double-blind review.

2. Anonymous authors, Title changed. "Dataset-Driven Study of Fine-Tuned LLMs for Security Bug Fixing Across Languages." Under double-blind review.

3. **Aayush Garg**, Constantinos Patsakis, Zanis Ali Khan, Qiang Tang. "Payload Analysis of Adversaries' Tooling: Automated Identification of Fuzzers." Under review.

4. Zanis Ali Khan, **Aayush Garg**, Yuejun Guo, Qiang Tang. "Evaluating Pre-Trained Models for Multi-Language Vulnerability Patching." Under review.

5. **Aayush Garg**, Renzo Degiovanni, Mike Papadakis, Yves Le Traon. "Vulnerability Mimicking Mutants." Under review.

6. **Aayush Garg**, Renzo Degiovanni, Matthieu Jimenez, Maxime Cordy, Mike Papadakis, Yves Le Traon. "Learning to Predict Vulnerabilities from Vulnerability-Fixes: A Machine Translation Approach." Under review.

References

Available upon request.