

Robert Podschwadt

E-Mail: rpodschwadt@gmail.com / rpodschw@odu.edu

Education

Phd **09/2019 - 12/2023**

Georgia State University

Dissertation:

Privacy-Preserving Deep Learning with Homomorphic Encryption: Addressing Challenges Related to Usability, Memory, and Recurrent Neural Networks

Area of research: Security in Machine Learning, Privacy Preserving Machine Learning

GPA: 4.25

Phd **09/2017 - 08/2019**

University of North Texas

Area of research: Security in Machine Learning

GPA: 4.0

Master of Science **09/2009-03/2012**

Hochschule der Medien Stuttgart, Computer Science and Media

Thesis: GPU aided Gaussian Process Regression in Python

Thesis grade: 1.3 [Very Good, American equivalent: A]

Overall grade: 1.5 [Very Good, American equivalent: A-]

Bachelor of Science **03/2006-07/2009**

Hochschule der Medien Stuttgart, Medieninformatik

Thesis: Implementation and visualization of selected AI algorithms in Python

Thesis grade: 1.1 [Very Good, American equivalent: A]

Overall grade: 1.9 [Good, American equivalent: A-]

Abitur (High School) **2005**

Kepler Gymnasium Freudenstadt

Final grade: 2.4 [Good, American equivalent: B+]

Publications

Memory Efficient Privacy-Preserving Machine Learning Based on Homomorphic Encryption

International Conference on Applied Cryptography and Network Security 2024

https://link.springer.com/chapter/10.1007/978-3-031-54773-7_13

Robert Podschwadt, Parsa Ghazvinian, Mohammad GhasemiGol, Daniel Takabi

A Survey of Deep Learning Architectures for Privacy-Preserving Machine Learning With Fully Homomorphic Encryption

IEEE Access 10, 117477-117500

<https://ieeexplore.ieee.org/abstract/document/9936637/>

Robert Podschwadt, Daniel Takabi, Peizhao Hu, Mohammad H Rafiei, Zhipeng Cai

Neurocrypt: Machine learning over encrypted distributed neuroimaging data

Neuroinformatics 20 (1), 91-108

<https://link.springer.com/article/10.1007/s12021-021-09525-8>

Nipuna Senanayake, Robert Podschwadt, Daniel Takabi, Vince D Calhoun, Sergey M Plis

Non-interactive privacy preserving recurrent neural network prediction with homomorphic encryption

2021 IEEE 14th International Conference on Cloud Computing (CLOUD)

<https://ieeexplore.ieee.org/abstract/document/9582263>

Robert Podschwadt and Daniel Takabi

Classification of Encrypted Word Embeddings using Recurrent Neural Networks

PrivateNLP 2020

http://ceur-ws.org/Vol-2573/PrivateNLP_Paper3.pdf

Robert Podschwadt and Daniel Takabi

Privacy preserving Neural Network Inference on Encrypted Data with GPUs

<https://arxiv.org/abs/1911.11377>

Daniel Takabi, Robert Podschwadt, Jeff Druce, Curt Wu, Kevin Procopio

Effectiveness of Adversarial Examples and Defenses for Malware Classification

SecureComm 2019

<https://arxiv.org/abs/1909.04778>

https://link.springer.com/chapter/10.1007/978-3-030-37231-6_22

Robert Podschwadt and Hassan Takabi

Projects

CryptoDL

ongoing

A library to perform inference over homomorphically encrypted data

<https://github.com/inspire-lab/CryptoDL>

Research and Work Experience

Research Assistant Professor

01/2024- present

Old Dominion University, Norfolk Virginia, USA

Research in usability and performance of privacy-preserving machine learning systems.

PhD Student

8/2019 - 12/2023

Georgia State University, Atlanta Georgia, USA

Research in using machine learning for security critical tasks and privacy preserving machine learning

PhD Student

8/2017 - 8/2019

University of North Texas, Denton TX, USA

Research in using machine learning for security critical tasks.

Training Workshop on Adversarial Machine Learning

12/10/2019

ACSAC 2019, Puerto Rico

https://www.openconf.org/acsac2019/modules/request.php?module=oc_program&action=page.php&id=58

Instructor of Upward Bound Summer Camp

7/2019

University of North Texas, Denton TX, USA

Developed and taught a one week summer camps for middle and high school children as part of the UNT's Upward Bound program. The goal of the camp was to teach the kids important cyber security concepts and how to behave ethically in the digital world.

(<https://trio.unt.edu/ub>)

Tutorial on Adversarial Machine Learning
ACSAC 2018, Puerto Rico

12/03/2018

https://podschwadt.github.io/aml_tutorial/

Instructor of GenCyber Summer Camp
University of North Texas, Denton TX, USA

6/2018 - 8/2018

Developed and taught five summer camps for middle and high school children as part of the GenCyber summer camps. The goal of the camps was to teach the kids important cyber security concepts and how to behave ethically in the digital world. (<https://www.gen-cyber.com/about/>)

System Developer

07/2012 - 08/2017

Sirrix Security Technologies/[Rohde & Schwarz Cybersecurity](#), Saarbrücken, Germany

[Sirrix](#) is a cutting-edge company in security software, recently acquired by Rohde und Schwarz. My responsibilities include:

- Implementation (in Java) of the [Sirrix.TrustedObjects Manager \(part of Trusted VPN\)](#), our highly parallel central management server. User input is transformed into desired configurations for all connected client systems, which are then distributed over TLS-secured connections. The server is configurable using web applications built with Ajax.
- Development and implementation of security concepts for new products, including the use of PKIs to establish trust, adaptation of the management server for new secure communications systems, and development of user-friendly configuration interfaces.
- Design of protocols for communication between clients and servers. These protocols need to allow for secure transmission of configuration data to client systems and offer callable services on either side.
- Overseeing the education of apprentices and student interns.

Researcher/Software Developer

03/2011-12/2011

Center for Solar Energy and Hydrogen Research Baden-Württemberg

Zentrum für Sonnenenergie- und Wasserstoff-Forschung (ZSW) Baden-Württemberg

(www.zsw-bw.de) is a state-funded research institute whose goal is to improve renewable energy systems.

- Completed Master's thesis in association with ZSW, supervised by Dr. Frank Sehnke.
- Thesis work involved developing a system to predict energy output of the power grid based on predictions made by a physics simulation. The prediction method of choice was Gaussian Processes. Part of the thesis was to evaluate the feasibility of using GPUs for the computation and to compare the Gaussian Process system to the existing neural network system with respect to speed and prediction quality.

Intern **09/2008–02/2009**
IBM Deutschland (Böblingen, Germany), System Automation department

- Designed and evaluated feasibility of a system for generating code templates from UML diagrams.

Intern **03/2008–08/2008**
IBM Deutschland (Böblingen, Germany), System Automation department

- Implemented features in a Java-based web application for process automation.

Skills

- Programming Languages: Java (expert), Python(expert), JavaScript (advanced), C/C++(expert), Machine learning, Keras, Tensorflow
- Platforms : Linux, Windows
- Databases: SQL, JDBC, Firebird, DB2
- Methodologies: SCRUM, Extreme Programming, SVN, Kanban, Public key infrastructure security concepts, Git
- Languages: German (native), English (fluent), French (beginning)