Message from the DSML Workshop Chairs
DSN-W 2024

It is our pleasure to welcome you to the 7th International Workshop on Dependable and Secure Machine Learning (DSML), co-located with the 54th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2024) in Brisbane, Australia on Monday, 24 June 2024.

Machine learning (ML) is increasingly used in critical domains, such as healthcare and wellness, criminal sentencing recommendations, commerce, and transportation. The design of ML-enabled systems has mainly focused on developing models, algorithms, and datasets on which they are trained to demonstrate high accuracy for specific tasks, such as object or speech recognition and classification. ML algorithms typically construct a model by training on a labeled training dataset and its performance is assessed based on the accuracy in predicting labels for unseen (but often similar) testing data. This is based on the assumption that the training dataset is representative of the inputs that the system will face in deployment. However, in practice there are a wide variety of unexpected, accidental, as well as maliciously crafted, perturbations to the inputs that might lead to violations of this assumption. ML models are also over-confident about their predictions when processing such unexpected inputs. This makes it difficult to deploy them in safety critical settings where one needs to be able to rely on the predictions to make decisions or revert back to a failsafe mode. ML models are often run on special-purpose hardware accelerators, which may themselves be subject to faults. As a result, there is a growing concern regarding the reliability, safety, security, and accountability of ML systems.

The DSML workshop is an open forum for researchers, practitioners, and regulatory experts, to present and discuss innovative ideas and practical techniques and tools for producing dependable and secure ML-enabled systems. A primary goal of the workshop is to draw the attention of the research community to the problem of establishing guarantees of reliability, security, safety, and robustness for systems that incorporate increasingly sophisticated ML models, and to the challenge of determining whether such systems can comply with requirements for safety-critical systems. A further goal is to build a research community at the intersection of machine learning and dependable and secure computing.

This year's workshop features five sessions, including two keynote sessions and research presentations. We had 9 paper submissions this year, of which we accepted 5 full papers, 2 short papers, and one research talk. The papers were selected by the technical program committee (TPC) based on reviews and online discussion. Each paper was reviewed by three TPC members. The workshop sessions are organized as follows:

The workshop will have two keynotes. The first keynote will be held in Session 1 which will feature Taylor Johnson from Vanderbilt University, USA. His talk will discuss formal methods for assuring specifications—mostly robustness and safety—in autonomous CPS and subcomponents. In Session 3, we will have the second keynote, featuring Guangdong Bai from the University of Queensland, Australia. His talk will focus on leveraging machine learning for privacy compliance in software ecosystems. The workshop will have Session 2, 4, and 5 covering the accepted papers. Session 2 will feature "Defense Mechanisms for Secure ML System", Session 4 will cover "Dependable and Reliable ML Systems", and the last season will cover "ML Systems for Security and Beyond."

Finally, we thank our TPC members for their collective efforts in reviewing the papers, and for helping us develop the workshop program. We also thank the organizers of the DSN conference for their support of the DSML workshop and the community for their valued contributions to the workshop.

Sanghyun Hong, *Oregon State University, USA*
Bo Fang, *Pacific Northwest National Laboratory, USA*