WOLF: Automated Machine Learning Workflow Management Framework for Malware Detection and Other Applications

Submitted by sanaawan on Fri, 03/13/2020 - 1:51pm. Contributors: Sohaib Kiani, Sana Awan, Fengjun Li, Bo Luo

Applying machine learning techniques to solve real-world problems is a highly iterative process. The process from idea to code and then to experiment may require up to thousands of iterations to find the optimum set of hyper-parameters. Also, it is hard to find best machine learning techniques for a given dataset. The WOLF framework has been designed to simultaneously automate the process of selecting the best algorithm and searching for the optimum hyper-parameters. It can be useful to both who are novice in machine learning and just want to find best algorithm for their dataset, and also to those who are experts in the field and want to compare their new features or algorithm with state of the art techniques. By incorporating the WOLF framework in their designs, it is easier for novices to apply machine learning techniques on their dataset. With a wide range of evaluation metrics provided, WOLF also helps data scientists to develop better intuition towards machine learning techniques and speed up the process of algorithm development. Another main feature of the WOLF framework is that user can easily integrate new algorithms at any stage of the machine learning pipeline. In this paper, we present the WOLF architecture, and demonstrate how it could be used for standard machine learning datasets and for Android malware detection tasks. Experimental results show the flexibility and performance of WOLF.

Sohaib Kiani is currently a PhD-Computer Science candidate in University of Kansas. His research interests include Adversarial Machine Learning and applications of machine learning algorithms for various security applications. He did his MS in Information Technology from RWTH Aachen, Germany and BS in Communication Engineering from NU-FAST Islamabad, Pakistan.

Sana Awan is currently a PhD-Computer Science Candidate in University of Kansas. Her area of research is Cybersecurity, particularly security in the Internet of Things domain. She designed and implemented network security solutions and intrusion detection systems that employ machine learning to improve security while maintaining reliability and continued deployment. She did her MS in System Engineering from University of Maryland, USA and BS in Electrical Engineering from NUST Islamabad, Pakistan.
Dr. Fengjun Li is an associate professor at the Department of Electrical Engineering and Computer Science of the University of Kansas. She received B.E. degree (with honor) from the University of Science and Technology of China in 2001, M.Phil. from the Chinese University of Hong Kong in 2004 and Ph.D. from the Pennsylvania State University in 2010. She received the Kansas NSF EPSCoR First Award in 2014, KU Miller Scholar Award in 2016 and KU Bellows Scholar Award in 2019. Her research interests lie in a broad area of security and privacy for distributed information systems, cyber-physical systems and communication networks.

Dr. Bo Luo is currently a full professor with the EECS department at the University of Kansas. He is the director of the Information Assurance Laboratory (IAL) at KU's Information and Telecommunication Technology Center (ITTC), which is a National Center of Academic Excellence in Cyber Defense designated by NSA and DHS. He was awarded the Miller Professional Development Award at KU in 2015, and the Miller Scholar awards in 2016 and 2017. He received Ph.D. degree from The Pennsylvania State University in 2008, M.Phil degree from the Chinese University of Hong Kong in 2003, and B.E. from University of Sciences and Technology of China in 2001.

License: Creative Commons 2.5

Other available formats:

WOLF: Automated Machine Learning Workflow Management Framework for Malware Detection and Other Applications
Switch to normal viewerSwitch to experimental viewer