1. DeepGauge: multi-granularity testing criteria for deep learning systems

Lei Ma (3); Juefei-Xu, F. (4); Fuyuan Zhang (1); Jiyuan Sun (2); Minhui Xue (1); Bo Li (5); Chunyang Chen (6); Ting Su (1); Li Li (6); Jianjun Zhao (2); Yadong Wang (3)
Source: *2018 33rd IEEE/ACM International Conference on Automated Software Engineering (ASE). Proceedings*, p 120-31, 2018; **ISBN-13:** 978-1-4503-5937-5; **DOI:** 10.1145/3238147.3238202; **Conference:** 2018 33rd IEEE/ACM International Conference on Automated Software Engineering (ASE), 3-7 Sept. 2018, Montpellier, France; **Sponsor:** ACM SIGSOFT; **Publisher:** IEEE, Piscataway, NJ, USA
Author affiliation: (1) Nanyang Technological University, Singapore (2) Kyushu University, Japan (3) Harbin Institute of Technology, China (4) Carnegie Mellon University, Pittsburgh, PA, United States (5) University of Illinois, Urbana, IL, United States (6) Monash University, Melbourne, VIC, Australia
Abstract: Deep learning (DL) defines a new data-driven programming paradigm that constructs the internal system logic of a crafted neuron network through a set of training data. We have seen wide adoption of DL in many safety-critical scenarios. However, a plethora of studies have shown that the state-of-the-art DL systems suffer from various vulnerabilities which can lead to severe consequences when applied to real-world applications. Currently, the testing adequacy of a DL system is usually measured by the accuracy of test data. Considering the limitation of accessible high quality test data, good accuracy performance on test data can hardly provide confidence to the testing adequacy and generality of DL systems. Unlike traditional software systems that have clear and controllable logic and functionality, the lack of interpretability in a DL system makes system analysis and defect detection difficult, which could potentially hinder its real-world deployment. In this paper, we propose DeepGauge, a set of multi-granularity testing criteria for DL systems, which aims at rendering a multi-faceted portrayal of the testbed. The in-depth evaluation of our proposed testing criteria is demonstrated on two well-known datasets, five DL systems, and with four state-of-the-art adversarial attack techniques against DL. The potential usefulness of DeepGauge sheds light on the construction of more generic and robust DL systems. (0 refs)
Inspec controlled terms: learning (artificial intelligence) - neural nets - program testing - safety-critical software - security of data
Uncontrolled terms: DeepGauge - multigranularity testing criteria - deep learning systems - data-driven programming paradigm - internal system logic - DL system - system analysis - defect detection - crafted neuron network
Classification Code: C6150G Diagnostic, testing, debugging and evaluating systems - C6170K Knowledge engineering techniques - C5290 Neural computing techniques - C6110B Software engineering techniques - C6130S Data security
IPC Code: G06F9/44 - G06F11/36 - G06F21/00 - G06N5/04 - G06N20/00
Treatment: Bibliography (BIB) - Practical (PRA)
Database: Inspec
Data Provider: Engineering Village