ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

TIỂU LUẬN

Một số vấn đề về đồ hoạ máy tính
Giám sát hệ thống micro-services và vấn đề logging

Đại học Quốc gia Hà Nội
Đại học Khoa học Tự nhiên
Khoa Toán cơ tin

Giảng viên: TS. Nguyễn Thị Bích Thuỷ

Học viên: Nguyễn Mạnh Linh, Nguyễn Đức Thịnh

Mục lục

Tóm tắt

Ngoài việc lập trình thì vận hành và giám sát là khâu quan trọng trong vòng đời của một sản phẩn công nghệ (phần mềm). Vận hành một sản phẩm không hề dễ dàng hơn việc tạo ra nó. Khi một phần mềm được triển khai thực tế, lập trình viên cũng như người quản trị hệ thống luôn cần nắm rõ *sức khoẻ* của sản phẩm ví dụ như phần mềm đang tiêu tốn bao nhiêu tài nguyên của máy tính, phần mềm xử lý yêu cầu nhanh hay chậm, hay có bao nhiêu lỗi xảy ra trong khung giờ... Những thông số hay độ đo này là thước đo để biết được sản phẩm có đủ tốt hoặc quan trọng hơn là cảnh báo sớm cho người làm phần mềm về những nguy cơ có thể xảy ra. Bài báo cáo này giới thiệu một loạt các kĩ thuật, độ đo, cách kết hợp những công cụ và việc vận dụng khéo léo giữa bản thân phần mềm (ghi log) và các công cụ đó. Trực quan hoá dữ liệu được sử dụng một cách triệt để nhằm tạo một cái nhìn từ tổng quan đến chi tiết giúp cho người vận hành hệ thống cũng như lập trình viên luôn giữ được phần mềm của mình trong tầm kiểm soát.

1 Giới thiệu

Trước hết, báo cáo này không phải một hướng dẫn cụ thể về cài đặt công cụ hay về một chuẩn mực nào đó trong thiết kế hay phát triển phần mềm. Nội dung báo cáo dựa trên kinh nghiệm thực tế của tác giả trong quá trình làm sản phẩm (phần mềm), vậy nên chúng tôi sẽ trình bày một cách *vui vẻ* và *gần gũi* thay vì sử dụng ngôn ngữ *hàn lâm*.

Có nhiều tiêu chuẩn để đánh giá một phần mềm là tốt hay không, ví dụ như hiệu năng cao, ít lỗi, sử dụng tài nguyên hiệu quả... Mỗi người hoặc mỗi sản phẩm có đặc thù riêng để đặt ra tiêu chuẩn riêng. Ngoài ra cũng không tồn tại một sản phẩm nào mà vừa phát triển nhanh vừa chạy ổn định (ít hoặc không có lỗi) lại có hiệu năng cao và sử dụng ít tài nguyên, chúng ta luôn phải đánh đổi. Nhưng điều đó không có nghĩa là chúng ta phải bỏ đi tiêu chuẩn nào đó mà không cố gắng làm cho phần mềm ngày một tốt hơn. Trước khi làm được điều đó, chí ít chúng ta cần phải nắm được phần mềm đang tệ hoặc tốt ở điểm nào. Giám sát hệ thống sinh ra từ đó.

Một hệ thống giám sát, cảnh báo tốt có khả năng chỉ ra những thông tin có giá trị một cách trực quan nhất để người quản trị có thể dựa vào đó để đưa ra định hướng phát triển hoặc sửa chữa những lỗi xảy ra trong phần mềm. Hơn nữa, khi đặt các ngưỡng cảnh báo một cách hợp lý, ta có thể ra phương án sớm để tăng tài nguyên khi hệ thống bị cao tải hoặc có thể biết được hệ thống đang bị tấn công hoặc bị lỗi để có kịch bản ứng cứu sớm.

Tài liệu tham khảo

[1] Chen, Pin-Yu, et al. "Ead: elastic-net attacks to deep neural networks via adversarial examples." Proceedings of the AAAI conference on artificial intelligence. Vol. 32. No. 1. 2018.

[2] Shao, Weijia, Fikret Sivrikaya, and Sahin Albayrak. "Optimistic Optimisation of Composite Objective with Exponentiated Update." (2022).

[3] Beck, Amir, and Marc Teboulle. "A fast iterative shrinkage-thresholding algorithm for linear inverse problems." SIAM journal on imaging sciences 2.1 (2009): 183-202.

[4] Candès, Emmanuel J., and Michael B. Wakin. "An introduction to compressive sampling." IEEE signal processing magazine 25.2 (2008): 21-30.

[5] Carlini, Nicholas, and David Wagner. "Adversarial examples are not easily detected: Bypassing ten detection methods." Proceedings of the 10th ACM workshop on artificial intelligence and security. 2017.

[6] Carlini, Nicholas, and David Wagner. "Towards evaluating the robustness of neural networks." 2017 ieee symposium on security and privacy (sp). Ieee, 2017.

[7] Dong, Yinpeng, et al. "Towards interpretable deep neural networks by leveraging adversarial examples." arXiv preprint arXiv:1708.05493 (2017).

[8] Duchi, John, and Yoram Singer. "Efficient online and batch learning using forward backward splitting." The Journal of Machine Learning Research 10 (2009): 2899-2934.

[9] Evtimov, Ivan, et al. "Robust physical-world attacks on machine learning models." arXiv preprint arXiv:1707.08945 2.3 (2017): 4.

[10] Feinman, Reuben, et al. "Detecting adversarial samples from artifacts." arXiv preprint arXiv:1703.00410 (2017).

[11] Fu, Haoying, et al. "Efficient minimization methods of mixed l2-l1 and l1-l1 norms for image restoration." SIAM Journal on Scientific computing 27.6 (2006): 1881-1902.

[12] Goodfellow, Ian J., Jonathon Shlens, and Christian Szegedy. "Explaining and harnessing adversarial examples." arXiv preprint arXiv:1412.6572 (2014).

[13] Grosse, Kathrin, et al. "On the (statistical) detection of adversarial examples." arXiv preprint arXiv:1702.06280 (2017).

[14] Hinton, Geoffrey, Oriol Vinyals, and Jeff Dean. "Distilling the knowledge in a neural network (2015)." arXiv preprint arXiv:1503.02531 2 (2015).

[15] Kingma, Diederik P., and Jimmy Ba. "Adam: A method for stochastic optimization." arXiv preprint arXiv:1412.6980 (2014).

[16] Koh, Pang Wei, and Percy Liang. "Understanding black-box predictions via influence functions." International conference on machine learning. PMLR, 2017.

[17] Kurakin, Alexey, Ian J. Goodfellow, and Samy Bengio. "Adversarial examples in the physical world." Artificial intelligence safety and security. Chapman and Hall/CRC, 2018. 99-112.

[18] Kurakin, Alexey, Ian Goodfellow, and Samy Bengio. "Adversarial machine learning at scale." arXiv preprint arXiv:1611.01236 (2016).

[19] Liu, Yanpei, et al. "Delving into transferable adversarial examples and black-box attacks." arXiv preprint arXiv:1611.02770 (2016).

[20] Lu, J.; Issaranon, T.; and Forsyth, D. 2017. Safetynet: Detecting and rejecting adversarial examples robustly

[21] Madry, Aleksander, et al. "Towards deep learning models resistant to adversarial attacks." arXiv preprint arXiv:1706.06083 (2017).

[22] Moosavi-Dezfooli, Seyed-Mohsen, et al. "Universal adversarial perturbations." Proceedings of the IEEE conference on computer vision and pattern recognition. 2017.

[23] Moosavi-Dezfooli, Seyed-Mohsen, Alhussein Fawzi, and Pascal Frossard. "Deepfool: a simple and accurate method to fool deep neural networks." Proceedings of the IEEE conference on computer vision and pattern recognition. 2016.

[24] Papernot, Nicolas, et al. "The limitations of deep learning in adversarial settings." 2016 IEEE European symposium on security and privacy (EuroS&P). IEEE, 2016.

[25] Papernot, Nicolas, et al. "Distillation as a defense to adversarial perturbations against deep neural networks." 2016 IEEE symposium on security and privacy (SP). IEEE, 2016.

[26] Papernot, Nicolas, et al. "Practical black-box attacks against machine learning." Proceedings of the 2017 ACM on Asia conference on computer and communications security. 2017.

[27] Parikh, Neal, and Stephen Boyd. "Proximal algorithms." Foundations and trends® in Optimization 1.3 (2014): 127-239.

[28] Szegedy, Christian, et al. "Intriguing properties of neural networks." arXiv preprint arXiv:1312.6199 (2013).

[29] Szegedy, Christian, et al. "Rethinking the inception architecture for computer vision." Proceedings of the IEEE conference on computer vision and pattern recognition. 2016.

[30] Tramèr, Florian, et al. "Ensemble adversarial training: Attacks and defenses." arXiv preprint arXiv:1705.07204 (2017).

[31] Xu, Weilin, David Evans, and Yanjun Qi. "Feature squeezing: Detecting adversarial examples in deep neural networks." arXiv preprint arXiv:1704.01155 (2017).

[32] Zantedeschi, Valentina, Maria-Irina Nicolae, and Ambrish Rawat. "Efficient defenses against adversarial attacks." Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security. 2017.

[33] Zheng, Stephan, et al. "Improving the robustness of deep neural networks via stability training." Proceedings of the ieee conference on computer vision and pattern recognition. 2016.

[34] Zou, Hui, and Trevor Hastie. "Regularization and variable selection via the elastic net." Journal of the royal statistical society: series B (statistical methodology) 67.2 (2005): 301-320.