Case Study-based Portable Hands-on Labware for Machine Learning in Cybersecurity

Hossain Shahriar[1], Michael Whitman[2], Dan Lo[3]
[1]Department of Information Technology, [2]Institute for Cybersecurity Workforce Development, [3]Department of Computer Science
Kennesaw State University
Marietta, GA, USA
{hshahria, mwhitman, dlo2}@kennesaw.edu

Fan Wu[4], Cassandra Thomas[4]
[4]Department of Computer Science
Tuskegee University
Tuskegee, AL, USA
{fwu, cthomas}@tuskegee.edu

ABSTRACT

Machine Learning (ML) analyzes, and processes data and develop patterns. In the case of cybersecurity, it helps to better analyze previous cyber attacks and develop proactive strategy to detect and prevent the security threats. Both ML and cybersecurity are important subjects in computing curriculum, but ML for cybersecurity is not well presented there. We design and develop case-study based portable labware on Google CoLab for ML to cybersecurity so that students can access and practice these hands-on labs anywhere and anytime without time tedious installation and configuration which will help students more focus on learning of concepts and getting more experience for hands-on problem solving skills.

CCS CONCEPTS

• **Applied computing → Education → Collaborative learning**

KEYWORDS

Colab, Machine Learning, Cybersecurity, Case Study, Portable lab

ACM Reference format:

Hossain Shahriar, Michael Whitman, Dan Lo, Fan Wu, Cassandra Thomas, 2020. Case Study based Portable Hands-on Labware for Machine Learning in Cybersecurity. *Proceedings of 2020 ACM Technical Symposium on Computer Science Education (SIGCSE'20), March 11-14, 2020, Portland, OR, USA.* ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/3328778.3372579

1 INTRODUCTION

Today the Machine Learning (ML) plays a very important role in cybersecurity. According to Information Data Corporation (IDC), Artificial Intelligence (AI) and ML will grow from $8 billion in 2016 to $79 billion by 2022 [1]. As shared by Google, 50-70% of emails on Gmail are spam. With ML algorithms, Google is making it possible to block such unwanted communication with 99% accuracy [2].

ML can assist cybersecurity professionals to analyze malicious patterns and behaviors, predict patterns with suitable algorithms. ML can help to prevent similar attacks and respond to attacks more proactively. Many popular ML algorithms (e.g., Naïve Bayes, regression analysis, deep learning) are currently being applied to cybersecurity to detect security flaws and threats. ML can be applied to complex datasets to predict malicious events.

Many schools offer ML and cybersecurity courses in their computing curriculum but application of ML to cybersecurity is not well presented in the current curriculum. Hands-on skills activities in cybersecurity education can benefit all types of learners by providing opportunities for all types of learners to observe as well as to perform [3]. We observe the scarce open source portable hands-on handy labware for ML for cybersecurity. The challenges in offering hands-on labs include the configuration of open source hands-on real labs; scarce dedicated staff and faculty in this field; and excessive time needed for developing open source materials. To overcome these difficulties, we develop case study-based, portable, modular, and easy-to-adopt labware.

Case study focuses on real world problems for analysis, requiring active participation to solve the problems. Our project explores Cybersecurity related Case Study with Google Colaboratory (CoLab) [4]. CoLab is a free notebook environment that requires no setup and runs entirely in the cloud. Each module in the Case study based portable hands-on labware mobile is designed based on a specific real-world cybersecurity case and consists of three components: pre-lab, hands-on lab, and post add-on lab. We implemented two labs (spam email detection and financial fraud prediction) and applied into classroom. The preliminary results and feedback showed that Case Study-based portable CoLab labware can increase learning confidence in ML and their application to cybersecurity problems.

REFERENCES

[1] IDC, https://www.idc.com/getdoc.jsp?containerId=prUS44911419, 2019
[2] F. Lardinois, Google Says its Machine Learning tech now blocks 99.9% of Gmail spam and phishing message, 2017, https://techcrunch.com/2017/05/31/google-says-its-machine-learning-tech-now-blocks-99-9-of-gmail-spam-and-phishing-messages/
[3] Why Hands-on Skills are Critical in Cyber Security Education, https://www.cybintsolutions.com/hands-on-skills-in-cyber-security-education/, 2018.
[4] CoLab, https://colab.research.google.com/notebooks/intro.ipynb

SIGCSE'20, March 11–14, 2020, Portland, OR, USA.

ACM ISBN 978-1-4503-6793-6/20/03
https://doi.org/10.1145/3328778.3372579