Coalescing Research into Modular and Safe Educational Cybersecurity Labs with AI Solutions

Tyler Judd*, Halil Bisgin*, Alvin Huseinovic†, Mohammad Derani‡ and Suleyman Uludag*
*Dept. of Comp. Sci., U. of Michigan-Flint, {tjudd,bisgin,uludag}@umich.edu,
† Faculty of Elect. Engin., U. of Sarajevo, Sarajevo, 71000 Bosnia & Herzegovina, ahuseinovic@etf.unsa.ba
‡ Dept. of Comp. Sci. and Engin., U. of Michigan - Ann Arbor, mderani@umich.edu

***Abstract*—Driven by a cybercrime industry worth over $6 trillion, the demand for cybersecurity professionals is surging with a projected increase of over 35% in jobs over the next decade according to the US Department of Labor's BLS. Simultaneously, advancements in Artificial Intelligence (AI), Data Science (DS), and Machine Learning (ML) are reshaping industries and creating challenges, notably job displacement for the under-skilled. This research-to-practice full paper addresses the critical need to integrate AI/DS/ML into cybersecurity education to meet these evolving demands.**

We envision a *marriage* of AI/DS/ML and cybersecurity (ADM4CYB) through a research-to-education paradigm. Despite extensive research, there remains a significant lack of publicly accessible labs that apply AI, DS, and ML to real-world cybersecurity challenges. As such, readily available, easy to adopt, modular, and hands-on labs applying AI/DS/ML solutions to cybersecurity problems are highly desirable.

At this juncture, we are developing a methodology that enables instructors and researchers to transform their work into practical, safe, and interactive teaching labs, enhancing student learning across various cybersecurity topics. Our initiative aims to integrate AI, DS, and ML techniques into interactive labs to effectively address current cybersecurity challenges. These modular labs provide students with both theoretical knowledge and hands-on experience, essential for adapting to the rapidly evolving field. By creating accessible labs, our methodology empowers students to develop skills across various cybersecurity topics. We also report results of our preliminary evaluation after using the first lab from this methodology in two classes that show increased learning, heightened levels of interest and motivation in the fields of networking, cybersecurity, AI/DS/ML, as well as coding.

***Index Terms*—Cybersecurity Labs, Containers, AI, Machine Learning, Data Science**

I. Introduction

Cybersecurity threats and cybercrime are the top technological global risks as identified by the World Economic Forum (WEF) in the organization's Global Risks Report 2024 Report [1]. Yet various state of cybersecurity reports [2], [3] from industry continue to indicate that accelerating cyber incidents, the increasing sophistication and persistence of threats [2], and more resources available to cybercriminals [4], create a threat landscape where defenders are unable to meet the challenge. To avoid dire financial and operational consequences, enhanced cybersecurity is viewed as a *changemaker* [5] for the resilience and reinvention of business in the 21^{st} century. Indeed, the cybersecurity market is experiencing a robust growth, with Figure 1 illustrating a significant increase (at least 50% annual budget growth) in global spending on cybersecurity solutions from 2016 to 2023 [7]. The market size for the worldwide information security products and services from 2015 to 2023 is illustrated in Figure 2. Thus, cybersecurity can be said to serve as one of the main pillars of any businesses' digital core and essentials to sustain a competitive advantage.

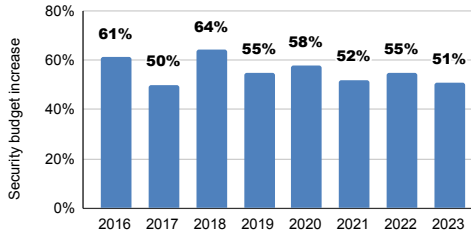

Fig. 1: Cyber security budget increase worldwide from 2016 to 2023 [6]. Companies worldwide have increased their security budgets by at least 50 percent annually since 2016.

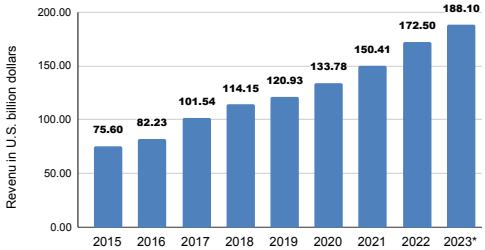

Fig. 2: Information security products and services market revenue worldwide from 2015 to 2023 [7].

The current workforce dynamics are exacerbated by the cybersecurity challenges of understaffed defenders and a persistent skills gap. According to the 2023 ISC2 Cybersecurity Workforce Study [8], the size of the global cybersecurity workforce hover around at 5.5 million - a 9% increase from 2022, and the highest ever recorded. The global workforce gap grew by 13% from 2022 to 2023, leading to roughly 4 million cybersecurity professionals shortage worldwide. Cybersecurity workforce gap by region is shown in Figure 3.

The US Department of Labor, BLS, Job Outlook handbook forecasts over 35% growth in cybersecurity positions in the next decade, highlighting the critical need for a significant expansion in qualified cybersecurity professionals. To complicate matters, the perennial workforce shortage and talent challenge

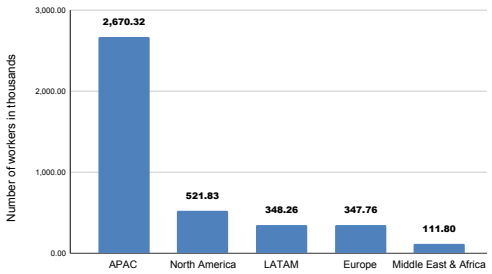

Fig. 3: CYB Workforce gap by region for 2023 [8].

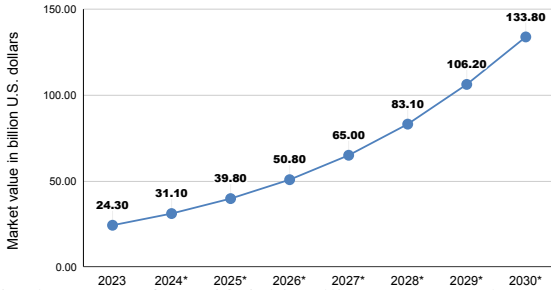

Fig. 5: The market for artificial intelligence (AI) cybersecurity.

remain at critical levels [9], and are even getting worse [10]. Recent reports indicate that the cybersecurity workforce gap has grown by 13% since just last year, with shortages reaching up to 2.6 million in the Asia-Pacific region alone [8]. As such, cybersecurity education, awareness, and training are top priority areas of investment for most companies [11]. New legislation is also moving forward with expanded cyber training and education through the Cybersecurity Awareness Act [12].

The generational disruptive technology of Artificial Intelligence (AI), together with its subareas of Machine Learning (ML) and Data Science (DS) in particular, are causing uprooting transformations in how we are conducting our businesses as well as our lives. According to Statista data shown in Figure 4, the AI market size is projected to rise from 241.8 billion U.S. dollars in 2023 to almost 740 billion U.S. dollars

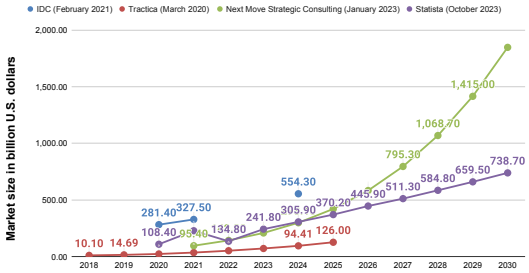

Fig. 4: Market size and revenue comparison for artificial intelligence worldwide from 2018 to 2030 [13].

in 2030, accounting for a compound annual growth rate of 17.3% [13].

Research indicates that integration of AI and cybersecurity has a huge potential. More specifically, the integration of AI into cybersecurity is becoming increasingly critical, as Figure 5 illustrates a significant growth trajectory in investments aimed at enhancing cyber defenses through advanced AI technologies. Indeed, current studies include a wide spectrum of applications ranging from malware analysis to intrusion detection for which several machine learning algorithms have been successfully leveraged. For example, Cyber AI is touted [14] as the real defense for augmenting cybersecurity with AI/ ML/ DS. Nevertheless, the transformation of such rich research resources into educational tools with a coupled curriculum, i.e., AI/ML/DS for cybersecurity (AMD4CYB), has not yet reached a desired level.

Although several attempts have been made to integrate AI into cybersecurity curricula, we are aware of no extensible or modular labs similar to the SEED labs from Syracuse University or labtainers from the Naval Postgraduate School in our topic. Our extensive survey of the literature, papers, books, courses, degrees, programs, certificates, lab exercises, projects, grants, tools, talks, and tutorials, simply does not show any combined approach of ADM4CYB. This highlights a significant gap in educational resources that effectively combine these critical areas, underscoring the need for the development of innovative, applicable educational materials.

Current attempts and efforts towards developing an ADM4CYB curriculum are in its infancy. As detailed in Section II, the pace of change in ADM4CYB and the proportional increase in the need for workforce and skill development have not been matched with educational materials. Our main contributions of our methodology we are proposing are as follows: (1) We base our use cases on actual peer-reviewed research papers, (2) We propose to develop a proof-of-concept for the aforementioned that anyone can apply, (3) We introduce a very critical aspect of data/attack generation into the educational material, (4) We provide a consistent and parameterized infrastructure based on virtual machines and docker containers, (5) We include auto-assessment for instructors, (6) We follow ABET Computing Accreditation Criteria, ACM CSEC 2017 Knowledge Areas, and NIST NICE competencies, (7) This lab we developed and deployed now is an initial phase of our long-term vision of developing material in this exciting area of ADM4CYB,

The rest of the paper is organized as follows: Section II reviews existing research on the application of AI/ML/DS in addressing cybersecurity threats, highlighting the breadth of the work while simultaneously noting its limited practical use in educational settings. Section III outlines the educational philosophies and accreditation standards driving the development of the ADM4CYB curriculum, emphasizing its foundation in active and experiential learning to advance cybersecurity education. Section IV outlines the approach for converting AI/ML/DS research papers into comprehensive research labs, while Section V demonstrates the practical application of this methodology through lab development, data preparation, deployment, and student interaction. Section VI presents an in-depth evaluation of the lab's impact on students, analyzing their enjoyment, motivation, and learning outcomes. Lastly,

Section VII provides detailed results and visual representations of data collected from student surveys, further demonstrating the lab's effectiveness in enhancing knowledge and interest in key areas of cybersecurity and machine learning.

II. Related Works

Extensive research efforts have been exerted on applying AI/ML/DS for cybersecurity problems [15]- [28], and these will likely continue at even higher levels. Besides the research publications, there are courses [29]- [36], a degree [37], a certificate [35], and books [38]- [46]. A list of tools and resources for machine learning for cybersecurity is also given in [47].

However, there is very limited published work on teaching and learning dimensions of AI/DS/ML for cybersecurity (ADM4CYB). In [48], an immersive learning environment is proposed on the Minecraft platform to visually expose students to insights of some of the machine learning techniques. A methodology to integrate AI and ML into cybersecurity curriculum is proposed in [49] after going over 5000 cybersecurity research papers in the literature, of which 78% mention AI terminology in them. Google Collab-based hands-on labware is explained at a high-level in [50]. However, we were not able to find any publicly available lab modules for general use.

As for the cybersecurity lab platforms, we note three commercial ones Hack The Box [51], NDG Online [52], and Try Hack Me [53]. Although these have good learning exercises, they are not freely and openly available to anyone. Although DETERLab [54]–[56] is an open testbed infrastructure for networking and cybersecurity experimentation and educational exercises, it is too complex for educational learning purposes, at least for the initial phase and we keep it in our future plans. EDURange was originally [57], [58] developed as a cloud-based framework for hosting on-demand cybersecurity scenarios for helping students develop analytical skills and security mindset. Now, it has moved from a cloud-based system to providing the full code [59] for anyone to install and maintain it [60]. There are a limited number of scenarios available and it is a rather heavy-lift to bring the system up and running. CyberStart provides a security education platform for younger adults through hacking challenges and puzzles [61], not a real lab platform. SEED Labs [62] are a collection of hands-on laboratory exercises for cybersecurity education [63], [64]. Again, SEED labs provide a good infrastructure but are beyond our scope for our initial phase of our project. Labtainers by Naval Postgraduate School [65] makes use of many of the SEED labs and develops a consistent and parameterizable cybersecurity lab infrastructure with automated assessment for use on individual student computers [66]–[68] built from docker containers.

To the best of our knowledge, none of the above materials addresses the focus of our work. By contrast, our goal is to use the labtainers infrastructure (virtual machines and dockers containers) to develop labs showing applications of machine learning techniques to major cybersecurity problems, where data generation for the attack scenarios will be fully implemented and realized in the labtainer platform.

III. Motivation

In this section, we present the motivation behind our development efforts from the pedagogical and ABET accreditation perspectives as well as providing a justification from the Knowledge Areas of the ACM CSEC 2017 [69].

A. Pedagogical

The main pillar of our pedagogy is based on Constructionist learning theories [70]–[72] by Papert, whose work grew from the constructivist theories of Jean Piaget. As noted in [73], Papert considers knowledge and learning to be firmly grounded in contexts, and shaped by their active and engaged uses. Our second pedagogical foundation is active learning as coined by Bonwell and Eison in [74]. Another pedagogical pillar is grounded in the Project-based learning methodology by Blumenfeld [75]. We believe that fostering student engagement and retention of learning are achieved by combining practices to pique student interest with a variety of challenging, authentic and real-world problem-solving tasks. Another objective is to transform students from passive learners to active learners by engaging them with intensive lab exercises. Intensive labs facilitate students' learning at the comprehension, application, synthesis and evaluation levels of cognition – the highest levels identified in Bloom's classic taxonomy [76], a framework about how people learn and its levels.

Other pillars of our pedagogical motivation are based on the following: (1) Experiential learning, developed by David Kolb [77], [78] with influences from John Dewey [79] who envisioned education as a journey of experiences rather than rote memorization, Kurt Lewin's Field Theory [80] who stated that behavior is the result of environment and the individual, and Jean Piaget's theory of cognitive development [81], (2) Authentic Learning, establish and maintain a true association between the classroom learning and the nature of the real world outside and beyond the classroom [82], [83], and (3) Active Learning [84], promoting competency development and higher cognitive thinking and activities, including metacognition, thinking about one's thinking, and reflection [85].

B. Curricular

Our College has made the commitment to get all its programs accredited by ABET, as an external validation of quality assurance and for developing and institutionalizing the continuous improvement process for teaching and learning. Our major goal through this project is to develop the labs and material to support ABET Accreditation Criteria [86] in cybersecurity, data science, and other computing programs. It is our goal to support the ABET's 6 crosscutting concepts of cybersecurity curriculum; that is confidentiality, integrity, availability, risk, adversarial thinking, and systems thinking. Further, ABET Curriculum Criteria (#5) requires the coverage of the following fundamental topics: (1) Data Sec., (2) Software Sec., (3) Component Sec., (4) Connection Sec., (5)

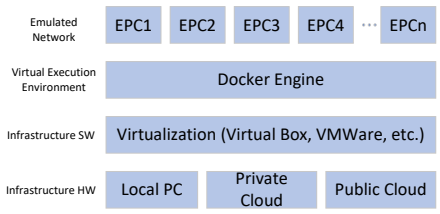

Fig. 6: Our lab architecture.

System Sec., (6) Human Sec., (7) Organizational Sec., and (8) Societal Sec. This project will give us a chance to start supporting and enabling all of these topics as well. Note that this project is an initial step towards our long-term goal of reaching the aforementioned ABET accreditation. In this project, we are only going to be addressing a small initial subset of the overarching goal.

Two other important references guiding us are the Knowledge Areas from ACM's CSEC 2017 [69] Knowledge Areas; competencies and work roles of the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework), Revision 1 [87] as well as its current update under revision [88].

IV. Methodology

We posit that any research paper applying an AI/ML/DS methodology to solve a cybersecurity problem can be converted into a teaching lab, assuming that students have some general familiarity with the basics of the corresponding AI/ML/DS techniques. Therefore, the framework we develop enables researchers or educators to develop their own labs. Figure 7 shows a high-level flowchart of our methodology for the *full cycle* of a complete lab.

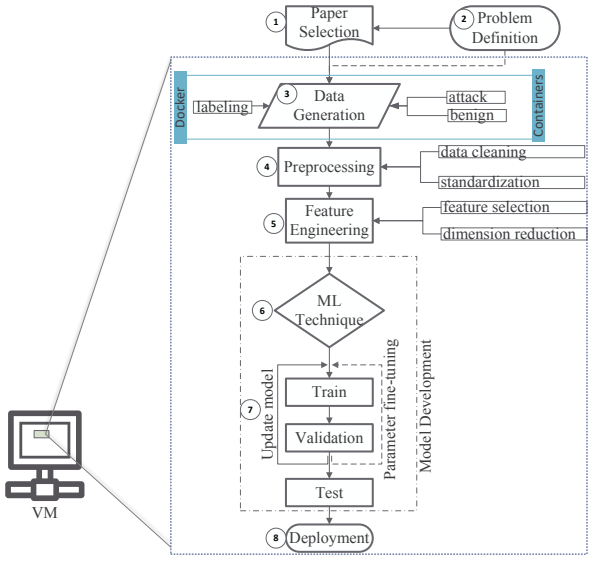

Fig. 7: Our Methodology.

Identifying a paper (Step 1 in Figure 7) that uses AI/ML/DS to address cybersecurity problems (Step 2 in Figure 7) is going to be our first step.

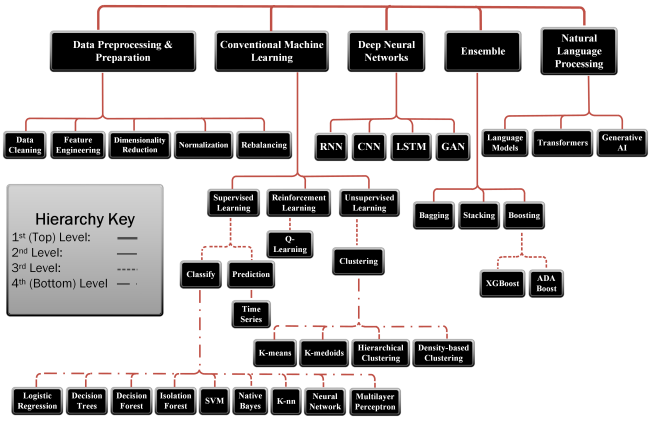

Fig. 8: Methods to address cybersecurity problems

Developing a defense solution for any attack scenario is only possible through a dataset (Step 3 in Figure 7), which often poses a challenge for reproducible research due to a lack of standardization [89]. To overcome this problem, we offer a virtual environment in our next step where users can build testbeds to generate the dataset required for the cybersecurity problem encountered. Hence, users can produce or simulate their own data with attack scenarios aligned with the guidelines in [89] and label them accordingly. The environment naturally allows users to exploit existing datasets which often come with the published work to be studied in the lab.

A data preprocessing step (Step 4 in Figure 7) is taken next to clean and standardize the data with the help of available tools in the literature, such as pcapML [89] or our in-house scripts. This is followed by a feature engineering (Step 5 in Figure 7) or selection method which can be again achieved by similar tools, such as nPrintML [90] in addition to our own preprocessing code base which will include the methods listed in the first branch of Figure 8.

After data preparation, a decision on which ML methods (Step 6 in Figure 7) should be applied can be made by considering the problem and the features available. Depending on the nature of the problem, we select solutions that can employ either conventional ML algorithms (supervised, unsupervised, and reinforcement learning) or Deep Learning (DL) approaches or natural language processing (NLP) methods some of which still be rooted in DL. In Figure 8, we present an organization of all methods we will consider for addressing cybersecurity challenges as part of our long term goals. Rather than present a comprehensive taxonomy of ML methods, our aim is to categorize and align these methods with the cybersecurity problems outlined in Figure 9.

Once an appropriate model is selected and the associated code is provided, *training* (Step 7 in Figure 7) can be performed on the data as the first step of the model development. To ensure the model's generalizability against future attacks, a *validation* or parameter tuning step can be incorporated. Finally, the deployment (Step 8 in Figure 7) concludes the

cycle in our framework.

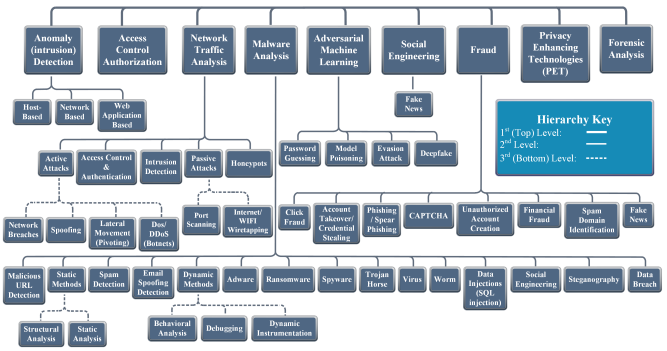

Fig. 9: The taxonomy of the cybersecurity problems we are planning to address over a long period of time.

V. Sample Development Lab

A. Labtainers

Our approach relies on modular labs, primarily utilizing Labtainers [65] developed by the Naval Postgraduate School [91]. Labtainers are modularized laboratory environments that students can access via a virtual machine. They provide a controlled setting for students to engage in various lab activities, irrespective of their operating system.

Accessing the Labtainers environment involves using a virtual machine and downloading the Labtainers base image.

The base image contains over 50 pre-installed labs, but what sets Labtainers apart and makes them particularly advantageous for our purposes is their flexibility. Users can create their own labs within the environment, which can then be readily downloaded onto other virtual machines that have the labtainer environment installed easily by students by just using a link. We will delve further into our utilization of this process in the creation of our lab.

B. Lab Developed

We have developed one lab fully following the procedure that is described in the following subsections, focusing on the detection of Domain over HTTP (DoH) vs traditional non-DoH traffic. In this lab, students are tasked with generating and capturing DoH and standard HTTP packets.

Subsequently, they utilize a traffic flow analyzer called Dohlyzer to extract crucial insights, which are then compiled into a .csv file. Students proceed to analyze this file and engage in various post-lab activities across different domains. For instance, for machine learning, they apply decision tree algorithms to examine and interpret the results. Additionally, for networking, they are required to manipulate DoH packet parameters and observe the resulting changes.

The lab was built within the Labtainer environment, providing modularity and accessibility to easily import into local or cloud-based virtual machines.

C. Process: Lab Creation

Once an instructor has selected a paper or topic they want to develop into a lab and laid out the necessary groundwork, including any data generation required for the lab to function they should start developing the lab outside of the Labtainer environment.

After creating the lab in an external environment, instructors can proceed to transition it to operate within the Labtainer environment. Instructors should first start by creating a new lab within their Labtainer environment, following the steps outlined in the Lab Designer Guide [92] published by the Naval Postgraduate School [91]. This guide offers in-depth insights into lab creation and contains a great deal of information regarding the Labtainer infrastructure. Subsequently, they should locate the Labtainer Dockerfile, which comprises all the necessary Linux packages for building the lab within the Labtainer environment. Instructors will add to this Dockerfile to incorporate their lab.

Furthermore, instructors must identify the specific libraries and scripts required for their lab and include them in the Dockerfile. The scripts can be incorporated into the Dockerfile by creating a GitHub repository, uploading the scripts, and cloning them into the Dockerfile. Instructors can then proceed to build the lab and address any encountered errors through debugging.

The creation process is outlined further in Figure 10

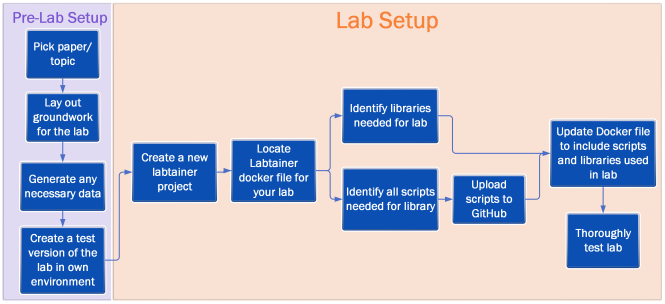

Fig. 10: Lab Creation Process

D. Process: Lab Exportation

Once instructors have tested their labs and are ready to start distributing them to their students, they can export the lab from the Labtainer environment. Initially, they need to create a Docker Hub repository to store the Dockerfile information for the lab. The repository name must follow the format *"[Docker Hub username]/[Lab name].[Lab name].student"* for the upload process to function correctly. Subsequently, the instructor also needs to establish a GitHub repository to house the main installation files.

Once these initial setup steps are completed, the instructor must locate the configuration file for the lab and input their Docker Hub username under the repository field. Additionally, they need to sign into their Docker Hub account within the Labtainer environment to upload to their Docker Hub account.

Instructors will then need to execute a series of commands to clean, package, and export the Labtainer images into their

Docker Hub repository. Following this, they will execute another series of commands to package the lab into a .tar file. Finally, the instructor will upload this file to their GitHub repository to enable students to download it using a link. These commands and steps are further outlined in section 10 of the Lab Designer Guide [92]. A high level representation of this process is outlined in Figure 11

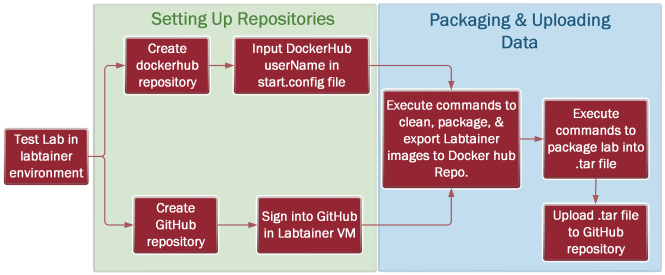

Fig. 11: Lab Exportation Process

E. Student Lab Usage

Before accessing the labs, students must ensure they have the necessary setup to utilize the Labtainer environment. Fortunately, a powerful machine is not required. There are several methods available for obtaining and setting up the Labtainer image. Students can install a virtual machine (VM) on their computer and download the Labtainer image, which requires approximately 5GB of storage. Alternatively, if storage space is limited, students can run Labtainer on a cloud-based service or use a pre-configured virtual machine provided by their organization in order to access the labtainer environment.

To access the labs, students will need to use the web URL obtained from the .tar file uploaded by the lab creator onto GitHub or a website of their choosing during lab exportation. Using this URL, combined with the `imodule` command, students can import the lab from GitHub or another web server onto their virtual machine. The command follows the format: `imodule <web URL>`. More information on 'imodules' can be found in Section 10 of the Lab Designer Guide [92].

Upon execution of the command, only configuration files will be downloaded onto the student's system. Students are then required to update the files and execute the lab. Once the lab is initiated, all inter component dependencies will be fetched from the Docker Hub repository established by the lab creator to store all necessary components. Students can then proceed to open and complete the lab. Figure 12 showcases the processes.

VI. Evaluation of Our First Lab

Given that our efforts have been at the intersection of machine learning and cybersecurity, we had two student cohorts from the Computer Networks and Data Mining courses for which the current lab could be appropriate to work on. While both groups of students were at the graduate level, their background varied. Nevertheless, they were assigned the lab and offered a virtual machine on which they were able to follow

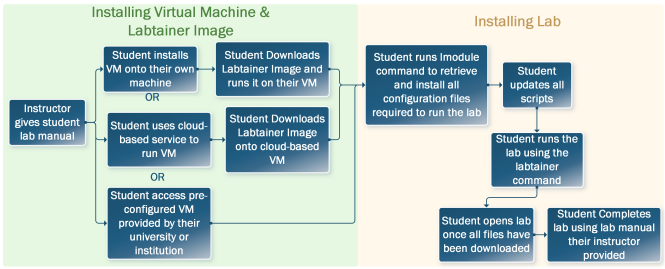

Fig. 12: Student Lab Usage

prescribed instructions which spanned preparation questions, network concepts, data simulation steps, and application of machine learning techniques.

After completion of the lab, students were given a survey which aimed to measure the effectiveness of the lab from nine different perspectives: demographics, research and internship experience, motivation, perception of the lab in general, lab setup, lab navigation, learning expansion, interest expansion, and suggestions for improvement.

As for the demographics, we further delved into students' background to see whether they were experienced in any of the topics that would not only include machine learning and cybersecurity, but also programming and networking in general. Related to that, students' previous experience in research or through an internship in these fields were possible indicators towards their success in the lab we wanted to measure. We also wanted to see if students were motivated enough to gain knowledge through a lab.

In order to see if the lab was pedagogically appealing or sound, we listed several questions about student perceptions such as their enjoyment level and understanding of instructions. These questions were followed with more technical aspects of the lab such as its setup procedure which might have sounded subtle for many. How to start the lab and interact with it might pose another barrier against student learning. Therefore, we sought student feedback on that aspect as well.

We also measured any improvements the lab may have contributed to student learning and interest. Both measures carry importance as we not only aim to teach related concepts where machine learning and cybersecurity meet, but also arise interest for a better learning environment.

Finally, we sought feedback from our students as to how we could improve our lab which would also inspire us for our future labs.

VII. Results

A. Student Demographics Analysis

Most students had a high-grade point average, with the lowest being 3.0, indicating strong academic commitment among participants. We also assessed their experience in major lab areas—Machine Learning/AI, Cybersecurity, Networking, and Programming and found that they had prior exposure to these subjects through different courses they have taken.

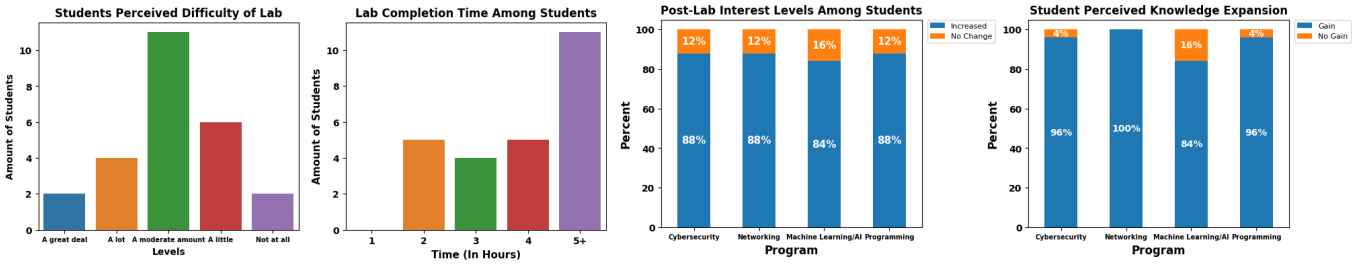

Fig. 13: Survey Results

B. Research and Internships Analysis

Most students lacked experience in research projects or internships related to the four main areas of study, with programming having the highest involvement. Experiences varied widely, ranging from professional development to university-specific projects, indicating diverse experience levels among students.

C. Lab Experience Analysis: Enjoyment, Motivation, Difficulty, and Time

Regarding the students' enjoyment levels post-lab, an overwhelming majority, 96 percent, expressed some degree of enjoyment, while only 4 percent reported none. This shows that most students enjoyed completing the lab. These findings are illustrated in Figure 14.

Similarly, motivation levels were high among students, with 96 percent indicating some degree of motivation to complete the lab. Many noted the opportunity to gain new skills and knowledge as significant contributors to their motivation.

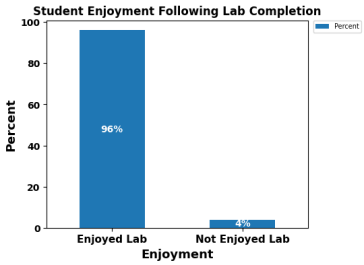

Fig. 14: Student Enjoyment

When assessing the perceived difficulty of the lab, most students rated it moderately challenging, with an average difficulty rating of 3.08 out of 5 with 5 being the most difficult. This suggests that while the lab presented challenges, they were manageable, as evidenced by the majority of students indicating they understood the tasks. Figure 13 further showcases these results.

In terms of time spent on the lab the responses indicated while most students understood all of the tasks it still took them awhile to complete the lab with the average time being around 4 hours with some taking longer. Despite understanding the tasks, the lab's complexity contributed to the extended completion times. Further insights into completion times are provided in Figure 13.

D. Lab Setup Analysis

Among the three methods provided for setting up their virtual machine (VCloud, Local PC, 3rd Party Service) to perform the labs, the majority of students opted for VCloud, which offered pre-configured virtual machines ready for connection. Alternatively, many students ran the labs on their local PCs. Only a single respondent reported using a third-party service for virtual machine setup.

E. Lab Performance Analysis

Initially, many respondents found that starting the lab was slightly challenging, but as they progressed, most students perceived it as fairly easy to navigate. Likewise, students reported that navigating the interface was not overly difficult. Regarding exporting deliverables, while some students found it slightly challenging, the majority understood the process and did not face many problems.

F. Learning Expansion and Interest Analysis

We asked students about if they had broadened their knowledge in the four main areas that the lab focuses on—Machine Learning/AI, CyberSecurity, Networking, and Programming. The results showed students showed a significant knowledge enrichment across all four areas, as demonstrated in Figure 13. Similarly, when asking students about their interest levels in each of the major areas after completing the lab, a majority reported an increased interest in these areas following lab completion. Figure 13 underscores this heightened interest.

Overall, the survey indicates that students largely enjoyed the lab, which, despite its time-consuming nature, was not overly challenging and students understood most, or all of the tasks assigned. Most notably, students gained both interest and knowledge in the lab's primary areas, highlighting its effectiveness in facilitating learning and engagement.

VIII. Conclusion and Future Work

Rapid developments in Artificial Intelligence (AI), Data Science (DS), and Machine Learning (ML) are transforming various sectors, often resulting in the displacement of less-skilled workers. This study discusses the urgent necessity to incorporate AI, DS, and ML into cybersecurity education to address these evolving needs.

Despite abundant research, there is a noticeable shortage of public labs that apply AI/DS/ML to tackle cybersecurity issues. Therefore, there is a strong demand for accessible, adaptable, modular, and practical labs that utilize AI/DS/ML

in addressing cybersecurity challenges. To this end, we suggest a synergistic integration of AI/DS/ML with cybersecurity (ADM4CYB) through a research-to-education approach.

We seek to embed AI, DS, and ML techniques within interactive labs to effectively confront current cybersecurity challenges. Our proposed methodology allows educators and researchers to convert their research into practical, safe, and interactive educational labs, thereby improving the learning experience across various cybersecurity themes. Our next labs will be converting our own publications in [93]–[95] . These modular labs equip students with both theoretical insights and practical skills, vital for keeping pace with the fast-changing domain. Our approach not only makes these labs widely accessible but also enables students to enhance their competencies in diverse cybersecurity areas. Additionally, initial assessments from implementing the first lab under this methodology in two classes indicate improved learning outcomes, and increased interest and motivation in networking, cybersecurity, AI/DS/ML, and programming.

IX. Acknowledgement

We would like to thank to Chris Wieringa for his technical support for creating the network simulation data.

References

[1] "The Global Risks Report 2024 19th Edition," World Economic Forum, Tech. Rep., January 2024. [Online]. Available: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

[2] "The State of Cybersecurity 2023, The Business Impact of Adversaries," Sophos, Tech. Rep., March 2023. [Online]. Available: https://www.sophos.com/en-us/whitepaper/state-of-cybersecurity

[3] "The State of Cybersecurity 2023," Splunk, Tech. Rep., April 2023. [Online]. Available: https://www.splunk.com/en_us/form/state-of-security.html

[4] "Global Cybersecurity Outlook 2023," World Economic Forum, Tech. Rep., January 2023. [Online]. Available: https://www.weforum.org/reports/global-cybersecurity-outlook-2023

[5] "State of Cybersecurity Resilience 2023," Accenture, Tech. Rep., June 2023. [Online]. Available: https://www.accenture.com/us-en/insights/security/state-cybersecurity

[6] Alexandra Borgeaud, "Cyber security budget increase worldwide from 2016 to 2023," Statista, Tech. Rep., 2023. [Online]. Available: https://www.statista.com/statistics/1322698/cybersecurity-budget-increase-forecast-worldwide/

[7] ——, "Information security products and services market revenu worldwide from 2015 to 2023," Statista, Tech. Rep., 2023. [Online]. Available: https://www.statista.com/statistics/305027/revenue-global-security-technology-and-services-market/

[8] "2023 ISC2 Cybersecurity Workforce Study ," ISC2, Tech. Rep., 2023. [Online]. Available: https://www.isc2.org/Insights/2023/10/ISC2-Reveals-Workforce-Growth-But-Record-Breaking-Gap-4-Million-Cybersecurity-Professionals

[9] "The State of Cybersecurity 2023," Splunk, Tech. Rep., April 2023. [Online]. Available: https://www.splunk.com/en_us/form/state-of-security.html

[10] "State of the Cybersecurity Workforce: New ISACA Research Shows Highest Retention Difficulties in Years," ISACA, Tech. Rep., March 2022. [Online]. Available: https://www.isaca.org/about-us/newsroom/press-releases/2022/state-of-the-cybersecurity-workforce-new-isaca-research-shows-retention-difficulties-in-years

[11] "State of the Cybersecurity 2023 Trends," Arctic Wolf, Tech. Rep., 2022. [Online]. Available: https://arcticwolf.com/the-state-of-cybersecurity-2023-trends/

[12] Sen. Gary Peters (D-MI), "S.1835 - National Cybersecurity Awareness Act, 118th Congress (2023-2024)," US Congress, Tech. Rep., 2023.

[13] Bergur Thormundsson, "Market size and revenue comparison for artificial intelligence worldwide from 2018 to 2030," Statista, Tech. Rep., 2024. [Online]. Available: https://www.statista.com/statistics/941835/artificial-intelligence-market-size-revenue-comparisons/

[14] "Tech Trends 2022: Cyber AI : Real Defense," Deloitte, Tech. Rep., 2022. [Online]. Available: https://www2.deloitte.com/us/en/insights/focus/tech-trends/2022/future-of-cybersecurity-and-ai.html

[15] D. Dasgupta, Z. Akhtar, and S. Sen, "Machine learning in cybersecurity: a comprehensive survey," *The Journal of Defense Modeling and Simulation*, vol. 19, no. 1, pp. 57–106, 2022.

[16] J. Martínez Torres, C. Iglesias Comesaña, and P. J. García-Nieto, "Machine learning techniques applied to cybersecurity," *Int'l Journal of Machine Learning and Cybernetics*, vol. 10, pp. 2823–2836, 2019.

[17] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, "A survey of deep learning methods for cyber security," *Information*, vol. 10, no. 4, p. 122, 2019.

[18] T. T. Nguyen and V. J. Reddi, "Deep reinforcement learning for cyber security," *IEEE Tran. on Neural Netw. and Learning Systems*, 2021.

[19] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, S. Chen, D. Liu, and J. Li, "Performance comparison and current challenges of using machine learning techniques in cybersecurity," *Energies*, vol. 13, no. 10, 2020.

[20] S. A. Salloum, M. Alshurideh, A. Elnagar, and K. Shaalan, "Machine learning and deep learning techniques for cybersecurity: a review," in *Proc. of the Int'l Conf. on AI and Comp. Vision*, 2020, pp. 50–57.

[21] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, "Machine learning and deep learning methods for cybersecurity," *Ieee access*, vol. 6, pp. 35 365–35 381, 2018.

[22] D. Priyanka and S. Sanjay, "Deep learning algorithms for cybersecurity applications: A technological and status review [j]," *Computer science review*, vol. 39, p. 100317, 2021.

[23] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications surveys & tutorials*, vol. 18, no. 2, pp. 1153–1176, 2015.

[24] S. Samtani, S. Yang, and H. Chen, "Acm kdd ai4cyber: The 1st workshop on artificial intelligence-enabled cybersecurity analytics," in *ACM SIGKDD*, 2021, pp. 4153–4154.

[25] S. Samtani, M. Kantarcioglu, and H. Chen, "Trailblazing the artificial intelligence for cybersecurity discipline: A multi-disciplinary research roadmap," *ACM Trans. Manage. Inf. Syst.*, vol. 11, no. 4, dec 2020.

[26] M. Abdelsalam, M. Gupta, and S. Mittal, "Artificial intelligence assisted malware analysis," in *Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems*, 2021, pp. 75–77.

[27] I. H. Sarker, A. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *Journal of Big data*, vol. 7, pp. 1–29, 2020.

[28] M. Musser and A. Garriott, "Machine learning and cybersecurity: Hype and reality," *Center for Security and Emerging Technology*, 2021.

[29] Taimur Ijlal, "Artificial Intelligence risk and cyber security course 2023," Udemy, Tech. Rep., 2023. [Online]. Available: https://www.udemy.com/course/artificial-intelligence-ai-governance-and-cyber-security/

[30] Hoang Quy La, "The Complete Artificial Intelligence for Cyber Security 2022," Udemy, Tech. Rep., 2022. [Online]. Available: https://www.udemy.com/course/the-complete-artificial-intelligence-for-cyber-security-2021/

[31] David Hoelzer, "SEC595: Applied Data Science and AI/Machine Learning for Cybersecurity Professionals," SANS, Tech. Rep. [Online]. Available: https://www.sans.org/cyber-security-courses/applied-data-science-machine-learning/

[32] "Applied Machine Learning for Cybersecurity," UC Berkeley, School of Information, Tech. Rep. [Online]. Available: https://ischoolonline.berkeley.edu/cybersecurity/curriculum/applied-machine-learning-for-cybersecurity/

[33] Ajit Jaokar and Raj Sharma, "Artificial Intelligence for Cyber Security," University of Oxford, Department of Continuing Education, Tech. Rep. [Online]. Available: https://www.conted.ox.ac.uk/courses/artificial-intelligence-for-cyber-security

[34] Emmanuel Tsukerman, "Cybersecurity Data Science," Udemy, Tech. Rep., 2020. [Online]. Available: https://www.udemy.com/course/cybersecurity-data-science/

[35] Yuxin Chen and Nick Feamster and Blase Ur , "Machine Learning for Cybersecurity," University of Chicago, Professional Education, Tech. Rep. [Online]. Available: https://professional.uchicago.edu/find-your-fit/professional-education/machine-learning-cybersecurity

[36] Kris Bolton, "Machine Learning for Security," Tech. Rep. [Online]. Available: https://security.kiwi/

[37] "Cybersecurity and Artificial Intelligence," University of Sheffield, Department of Computer Science, Faculty of Engineering, Tech. Rep. [Online]. Available: https://www.sheffield.ac.uk/postgraduate/taught/courses/2023/cybersecurity-and-artificial-intelligence-msc

[38] S. Dua and X. Du, *Data mining and machine learning in cybersecurity*. CRC press, 2011.

[39] M. A. Maloof, *Machine learning and data mining for computer security: methods and applications*. Springer, 2006.

[40] C. Chio and D. Freeman, *Machine learning and security: Protecting systems with data and algorithms*. " O'Reilly Media, Inc.", 2018.

[41] S. Halder and S. Ozdemir, *Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem*. Packt Publishing Ltd, 2018.

[42] A. Parisi, *Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies*. Packt Publishing Ltd, 2019.

[43] C. Chebbi, *Mastering machine learning for penetration testing: develop an extensive skill set to break self-learning systems using Python*. Packt Publishing Ltd, 2018.

[44] M. Stamp, C. A. Visaggio, F. Mercaldo, and F. Di Troia, *Cybersecurity for Artificial Intelligence*. Springer, 2022.

[45] C. D. S. Team *et al.*, "Introduction to artificial intelligence for security professionals," 2017.

[46] D. K. Bhattacharyya and J. K. Kalita, *Network anomaly detection: A machine learning perspective*. Crc Press, 2013.

[47] "Awesome Machine Learning for Cyber Security." [Online]. Available: https://github.com/jivoi/awesome-ml-for-cybersecurity

[48] J. Wei-Kocsis, M. Sabounchi, B. Yang, and T. Zhang, "Cybersecurity education in the age of artificial intelligence: A novel proactive and collaborative learning paradigm," in *IEEE FIE*, 2022, pp. 1–5.

[49] A. Aris, A. Uluagac, L. P. Rondon, D. Ortiz, M. Ross, and M. Finlayson, "Integrating artificial intelligence into cybersecurity curriculum: New perspectives," in *ASEE Annual Conf. & Expo*, 2022.

[50] D. Lo, H. Shahriar, K. Qian, M. Whitman, and F. Wu, "Colab cloud based portable and shareable hands-on labware for machine learning to cybersecurity," in *IEEE Int'l Conf on Big Data*, 2021, pp. 3311–3315.

[51] "Hack the box : Cybersecurity software web platform." [Online]. Available: https://www.hackthebox.com/

[52] "Network development group (ndg) online." [Online]. Available: https://www.netdevgroup.com/online/courses/cybersecurity

[53] "Try hack me : hands-on cyber security training platform." [Online]. Available: https://tryhackme.com/

[54] J. Mirkovic and T. Benzel, "Teaching cybersecurity with deterlab," *IEEE Security & Privacy*, vol. 10, no. 1, pp. 73–76, 2012.

[55] T. Benzel, "The science of cyber security experimentation: The deter project," in *Proc. of the Computer Security Applications Conference*, ser. ACSAC '11, 2011, p. 137–148. [Online]. Available: https://doi.org/10.1145/2076732.2076752

[56] J. Mirkovic, T. V. Benzel, T. Faber, R. Braden, J. T. Wroclawski, and S. Schwab, "The deter project: Advancing the science of cyber security experimentation and test," in *IEEE Int'l Conf on Technologies for Homeland Security (HST)*, 2010, pp. 1–7.

[57] R. Weiss, F. Turbak, J. Mache, and M. E. Locasto, "Cybersecurity education and assessment in edurange," *IEEE Security & Privacy*, vol. 15, no. 03, pp. 90–95, 2017.

[58] R. S. Weiss, S. Boesen, J. F. Sullivan, M. E. Locasto, J. Mache, and E. Nilsen, "Teaching cybersecurity analysis skills in the cloud," in *ACM SIGCSE*, 2015, pp. 332–337.

[59] "Edurange framework and code." [Online]. Available: https://github.com/edurange/edurange-flask

[60] "Edurange." [Online]. Available: http://www.edurange.org/

[61] "Cyberstart." [Online]. Available: https://cyberstart.com/

[62] "Seed labs." [Online]. Available: https://seedsecuritylabs.org/

[63] W. Du, "Seed: hands-on lab exercises for computer security education," *IEEE Security & Privacy*, vol. 9, no. 5, pp. 70–73, 2011.

[64] ——, *Computer & Internet Security: A Hands-on Approach, 3rd ed.* Wenliang Du, 2022.

[65] "Labtainers - cybersecurity lab exercises." [Online]. Available: https://nps.edu/web/c3o/labtainers

[66] C. E. Irvine, M. F. Thompson, M. McCarrin, and J. Khosalim, "Labtainers: a docker-based framework for cybersecurity labs," in *Proc. 2017 USENIX Workshop on Advances in Security Education*, 2017.

[67] C. E. Irvine, M. F. Thompson, and J. Khosalim, "Labtainers: a framework for parameterized cybersecurity labs using containers," 2017.

[68] M. F. Thompson and C. E. Irvine, "Individualizing cybersecurity lab exercises with labtainers," *IEEE Sec & Priv*, vol. 16, no. 2, pp. 91–95, 2018.

[69] "ACM/IEEE/AIS SIGSEC/IFIP Cybersecurity Curricular Guideline," 2017. [Online]. Available: https://cybered.hosting.acm.org/wp/

[70] S. Papert and I. Harel, *Constructionism*. Norwood: Ablex Publishing Corporation, 1991.

[71] I. Harel and S. Papert, *Constructionism*, I. Harel and S. Papert, Eds. Norwood, NJ: Ablex, 1991.

[72] S. Papert, "Situating constructionism," in *Constructionism*, I. Harel and S. Papert, Eds. Norwood, NJ: Ablex, 1991, pp. 1–12.

[73] E. Ackermann, "Piaget's constructivism, papert's constructionism: What's the difference?" in *Constructivism: Uses and Perspectives in Education Conference Proceedings*, Sep 2001, pp. 85–94.

[74] C. C. Bonwell and J. A. Eison, *Active learning : creating excitement in the classroom*. George Washington University, ERIC Clearinghouse on Higher Education, Washington, DC :, 1991.

[75] P. C. Blumenfeld, E. Soloway, R. W. Marx, J. S. Krajcik, M. Guzdial, and A. Palincsar, "Motivating project-based learning: Sustaining the doing, supporting the learning," *Educational Psychologist*, vol. 26, 1991.

[76] B. S. Bloom and D. R. Krathwohl, *Taxonomy of Educational Objectives, Handbook 1: Cognitive Domain*. Addison Wesley Publishing Company, October 1956.

[77] D. A. Kolb, R. E. Boyatzis, and C. Mainemelis, "Experiential learning theory: Previous research and new directions," in *Perspectives on thinking, learning, and cognitive styles*. Routledge, 2014, pp. 227–248.

[78] D. A. Kolb, *Experiential learning: Experience as the source of learning and development*. FT press, 2014.

[79] J. Dewey, "Experience and education," in *The educational forum*, vol. 50, no. 3. Taylor & Francis, 1986, pp. 241–252.

[80] K. Lewin, "Field theory in social science: selected theoretical papers (edited by dorwin cartwright.)." 1951.

[81] J. Piaget, *Origin of Intelligence in the Child: Selected Works vol 3*. Routledge, 2013, vol. 3.

[82] S. J. Stein, G. Isaacs, and T. Andrews, "Incorporating authentic learning experiences within a university course," *Studies in Higher Education*, vol. 29, no. 2, pp. 239–258, 2004.

[83] B. Van Oers and W. Wardekker, "On becoming an authentic learner: Semiotic activity in the early grades," *Journal of curriculum studies*, vol. 31, no. 2, pp. 229–249, 1999.

[84] M. Prince, "Does active learning work? a review of the research," *Journal of engineering education*, vol. 93, no. 3, pp. 223–231, 2004.

[85] C. Brame, "Active learning," *Vanderbilt University Center for Teaching*, 2016.

[86] "Criteria for Accrediting Computing Programs, 2023 – 2024," 2023. [Online]. Available: https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2023-2024/

[87] "NIST National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity," National Institute of Standards and Technology, Tech. Rep., November 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final

[88] "NIST National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity ," NIST, Tech. Rep., June 2023. [Online]. Available: https://www.nist.gov/document/nice-framework-work-role-categories-and-work-roles-introduction-and-summary-proposed

[89] J. Holland, P. Schmitt, P. Mittal, and N. Feamster, "Towards reproducible network traffic analysis," 2022.

[90] J. Holland, P. Schmitt, N. Feamster, and P. Mittal, "New directions in automated traffic analysis," in *ACM SIGSAC*, 2021, pp. 3366–3383.

[91] "Naval Postgraduate School." [Online]. Available: https://nps.edu/

[92] *Labtainer Lab Designer User Guide*, Naval Postgraduate School, 2022.

[93] Sadhvi C Narayanan and S. Uludag, "Two-tier anomaly detection for an internet of things network," in *IEEE CCNC*, January 2023, pp. 325–328.

[94] Yusuf Korkmaz, Alvin Huseinović, H. Bisgin, S. Mrdovic, and S. Uludag, "Using deep learning for detecting mirroring attacks on smart grid PMU networks," in *Int'l Balkan Conf. on Comm. and Netw. (BalkanCom)*, Aug 2022.

[95] Huseinovic, Alvin, Korkmaz, Yusuf, H. Bisgin, S. Mrdovic, and S. Uludag, "PMU Spoof Detection via Image Classification Methodology against Repeated Value Attacks by using Deep Learning," in *28th Int'l Conf. on Info., Comm. and Automation Techn. (ICAT)*, June 2022.