2026 ASEE ANNUAL CONFERENCE June 21–24, 2026 | Charlotte Convention Center, NC
Host Sponsor UNC Charlotte
ASEE AMERICAN SOCIETY FOR ENGINEERING EDUCATION
Paper ID #51859

GenAI-PassLab: Advancing Password Security Learning Through Generative AI

Mr. Tyler Earl Judd, University of Michigan
Oguz Kagnici, Bogazici University
Ali Arslan, University of Michigan - Flint

Ali Arslan is a researcher with interests in cybersecurity and applied machine learning. His work broadly explores data-driven security analysis and responsible use of computational methods. He is currently focused on advancing reproducible and ethical research practices

Alvin Huseinovic
Grace LaBelle, University of Michigan
Dr. Halil Bisgin, University of Michigan - Flint
Prof. Suleyman Uludag, University of Michigan

GenAI-PassLab: Advancing Password Security Learning Through Generative AI

Abstract

Artificial Intelligence and cybersecurity are converging rapidly, yet cybersecurity education has not kept pace, particularly in equipping students with hands-on experience at the intersection of machine learning, data science, and security. This paper introduces **GenAI-PassLab**, a modular, research-informed laboratory advancing password security education through generative AI. The lab enables students to engage with Large Language Models (LLMs) for password generation, strength evaluation, and adversarial analysis, connecting recent research to practical cybersecurity instruction.

GenAI-PassLab addresses a longstanding gap in computing curricula: the lack of applied laboratory infrastructure for teaching AI-enhanced cybersecurity, what we term *AI/ML/DS for Cybersecurity* (AMD4CYB). While platforms such as SEED Labs and Labtainers have advanced cybersecurity pedagogy, few integrate LLM-driven methods for password research. GenAI-PassLab fills this niche by allowing students to explore how AI models learn and replicate human password patterns, assess model behavior, and evaluate password strength using both heuristic and AI-based tools.

Implemented using the Labtainers containerization platform, the lab deploys custom GPT-2 models trained on real-world datasets including RockYou and Have I Been Pwned (HIBP). The lab manual includes pre-lab assessments, structured walkthroughs, and post-lab activities aligned with ABET, ACM CSEC 2017, and NIST NICE competencies.

Classroom deployments in upper-level undergraduate courses demonstrate strong outcomes: 100% of students reported expanded cybersecurity knowledge, 94% reported expanded AI knowledge, and the majority reported heightened awareness of real-world password vulnerabilities. The lab averaged a difficulty rating of 2.77 out of 5 and a completion time of 3.5 hours. These results position **GenAI-PassLab** as a scalable, research-aligned tool and a foundational component of a broader AMD4CYB lab ecosystem bridging AI research and cybersecurity pedagogy.

1 Introduction

Cybersecurity remains a critical global concern and is consistently ranked among the most significant technological risks by the World Economic Forum (WEF), as highlighted in its 2024 Global Risks Report [1]. Despite growing awareness and investment, the frequency, complexity, and persistence of cyber threats continue to outpace defense mechanisms [2, 3, 4]. Industry reports warn of an increasingly hostile threat landscape, wherein cybercriminals benefit from abundant tools and resources, widening the gap between offensive and defensive capabilities. Cybersecurity is now widely recognized as a strategic imperative and a catalyst for resilience, innovation, and competitive advantage in the digital economy [5].

Figure 1 illustrates the expanding market for information security products and services, underscoring cybersecurity's pivotal role in digital infrastructure.

Yet, this growth is shadowed by a persistent workforce crisis. The 2023 ISC2 Cybersecurity Workforce Study [7] estimates the global cybersecurity workforce at 5.5 million, up 9% from the

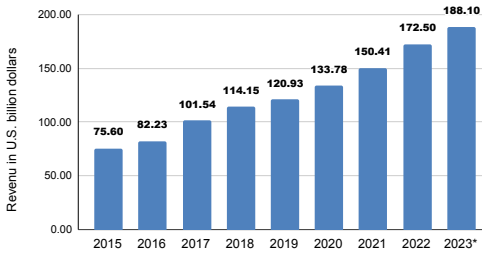


Figure 1: Market revenue for information security products and services worldwide from 2015 to 2023 [6].

previous year, but still leaves a staggering shortfall of over 4 million professionals. Figure 2 depicts this global talent gap, with regions like Asia-Pacific facing the steepest shortages.

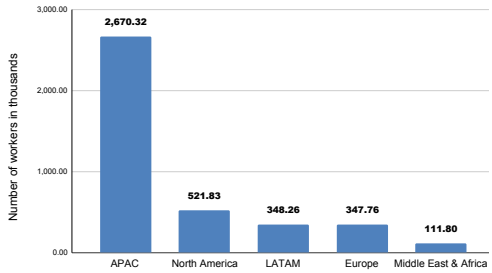


Figure 2: Cybersecurity workforce gap by region (2023) [7].

The U.S. Bureau of Labor Statistics projects a 33% increase in demand for cybersecurity roles over the next decade. However, this need is compounded by chronic underemployment, talent attrition, and training bottlenecks [8, 9]. In response, both the private and public sectors are prioritizing cybersecurity education, as seen in legislative initiatives like the Cybersecurity Awareness Act [10] and expanded corporate training investments [11].

Concurrently, artificial intelligence (AI) with its subfields of machine learning (ML) and data science (DS) has emerged as a disruptive force reshaping industries. As shown in Figure 3, the global AI market is projected to grow from $241.8 billion in 2023 to nearly $740 billion by 2030 [12].

The intersection of AI and cybersecurity offers transformative potential. Investment in AI-driven cybersecurity is accelerating rapidly, as shown in Figure 4, with the AI cybersecurity market expected to grow more than fivefold by 2030.

AI-powered solutions are already demonstrating their value in malware detection, intrusion prevention, and anomaly analysis [14]. However, despite promising research, these innovations have yet to be systematically translated into educational curricula. Particularly lacking is an integrated framework for teaching AI, ML, and DS in the context of cybersecurity, what we term *AMD4CYB*.

Positioning of AMD4CYB The AMD4CYB framing introduced in this work is intended as a curricular and pedagogical lens rather than as a standalone national initiative or alternative to

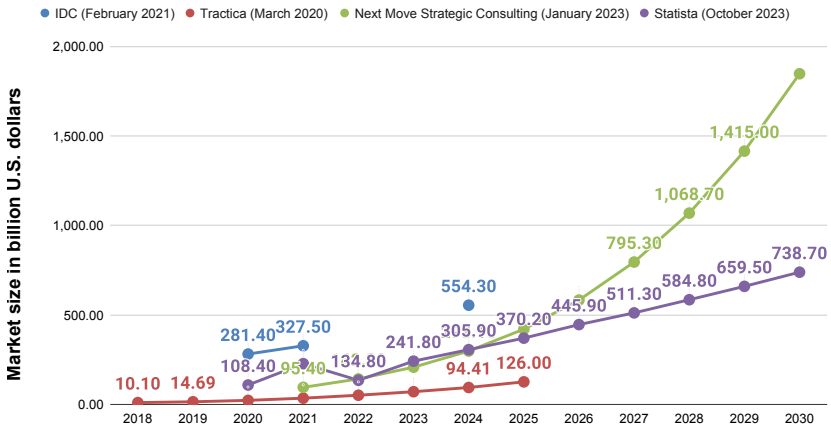


Figure 3: Worldwide AI market size from 2018 to 2030 [12].

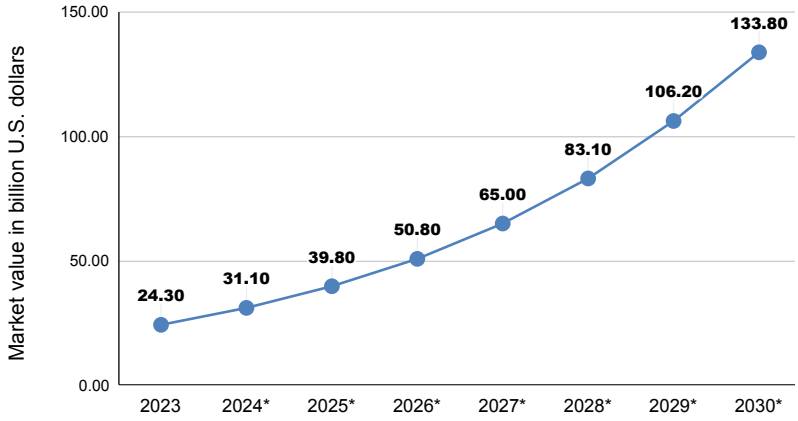


Figure 4: Projected growth of the AI cybersecurity market (2023–2030) [13].

existing programs. It aligns with broader efforts such as NSF- and NSA-supported CyberAI initiatives by emphasizing the integration of artificial intelligence, machine learning, and data science concepts within cybersecurity education. AMD4CYB complements these efforts by focusing specifically on course-level instructional design and hands-on laboratory experiences that can be adopted incrementally within existing curricula. In this sense, AMD4CYB serves as a localized, practice-oriented instantiation of broader educational priorities rather than a competing framework.

To date, there are no widely adopted lab infrastructures that integrate AMD4CYB concepts in a modular and extensible manner. While successful initiatives like SEED labs [15] and Labtainers [16] exist for general cybersecurity training, no such resources address AMD4CYB comprehensively. Our extensive survey across published literature, academic courses, online certificates, government and industry grants, educational tools, and community tutorials confirms this gap.

Although some pioneering efforts toward AMD4CYB curricula are underway, they remain fragmented and immature. As discussed further in Section 3, the pace of curricular innovation has not kept up with the urgency for skilling the future cybersecurity workforce.

Our contribution in this paper is the introduction of **GenAI-PassLab**, a novel, research-driven

cybersecurity lab that empowers learners to explore password generation using generative AI techniques. To the best of our knowledge, this is the first hands-on lab focused specifically on password generation using generative AI, and one of the first to extend AMD4CYB into classroom-ready, modular materials.

Our lab builds on principles outlined in our prior work [17], where we translated peer-reviewed research into tangible educational experiences. GenAI-PassLab continues this mission by offering:
(1) Real-world relevance: Use cases are grounded in published academic research and reflect practical password security challenges.
(2) Open and extensible infrastructure: Labs are implemented using virtual machines and Docker containers to ensure reproducibility and scalability.
(3) Dynamic content generation: Learners interact with and analyze AI-generated passwords using modern prompting techniques and evaluation metrics.
(4) Standards alignment: Materials map to ABET Computing Accreditation Criteria, ACM CSEC 2017 Knowledge Areas, and NIST NICE competencies.

GenAI-PassLab represents the initial phase of our broader vision: to develop a comprehensive suite of AMD4CYB labs that bridge the gap between cutting-edge research and accessible, high-impact cybersecurity education.

While the broader challenges of cybersecurity education and authentication technologies are well documented, this paper intentionally limits its scope to a single, focused instructional experience centered on password-based authentication. Passwords remain a widely deployed mechanism in practice and a useful pedagogical entry point for examining adversarial behavior, generative modeling, and ethical considerations in cybersecurity education. Accordingly, the remainder of the paper prioritizes the design and classroom use of the GenAI-PassLab experience over an exhaustive treatment of alternative authentication mechanisms.

Educational Goals
The design of GenAI-PassLab is guided by the following educational goals:

- **G1:** Enable students to understand how generative language models can be applied to password generation and adversarial security analysis.
- **G2:** Help students compare traditional heuristic-based password strength evaluators with AI-based approaches, and reason about the strengths and limitations of each.
- **G3:** Develop student intuition about how model architecture, training data, and training conditions influence the quality and security properties of generated passwords.
- **G4:** Promote ethical awareness regarding the use of leaked or real-world password datasets, including considerations of privacy, consent, and responsible data handling.

The rest of the paper is organized as follows: Section 2 provides the background about password security. A brief discussion of the related work is presented in Section 3. Section 4 elaborates on GenAI-PassLab. Evaluation of the lab through a survey from computing students is given in Section 5 with findings in Section 6. Concluding remarks are in Section 7.

2 Background

Prior work has extensively documented the importance of hands-on cybersecurity education, the persistent challenges of password-based authentication, and the growing influence of artificial intelligence in security contexts. Rather than reproducing this body of work in full, this section briefly situates GenAI-PassLab within three intersecting strands of literature: (1) experiential cybersecurity education, (2) pedagogical approaches to teaching password security and adversarial thinking, and (3) emerging uses of generative models in computing education. This focused review provides the necessary context for the lab design while allowing the paper to concentrate on the instructional experience itself.

Password security remains a cornerstone of digital authentication, yet decades of real-world breaches expose ongoing failures in storage practices, user behavior, and system design. Despite the rise of multi-factor authentication and biometrics, passwords continue to dominate due to their ease of implementation and user familiarity.

Over the past two decades, high-profile data breaches have repeatedly highlighted these issues. In 2007, hackers extracted plaintext usernames, emails, and passwords from over 250,000 users of the gambling platform FoxyBingo. MySpace's 2008 breach affected over 350 million users, where passwords were hashed using a flawed SHA1 implementation that truncated them to 10 characters and converted all uppercase characters to lowercase. In 2009, the MoneyBookers breach exposed 4.5 million accounts, including sensitive recovery questions [18]. Gawker Media's 2010 breach exposed over 1.3 million credentials, where only the first eight characters of passwords were encrypted, allowing attackers to reconstruct access using source code leaked from internal servers [19]. These examples reveal systemic weaknesses in how passwords are stored and processed.

Datasets from such breaches are now central to both offensive and defensive security research. Sites like `haveibeenpwned.com`, developed by Troy Hunt, allow users to search their email addresses to determine breach exposure. On the attacker side, massive dictionaries like RockYou2021 (8.5B passwords) and RockYou2024 (9.9B passwords) [20] are widely used for brute-force attacks and statistical modeling. Table 1 summarizes common passwords by length from the 2025 Specops report [21].

These insights into weak password usage have spurred tools like HashCat, which uses rule-based transformations to crack passwords. However, traditional approaches are constrained by predefined dictionaries and static heuristics. Recent advances in machine learning, particularly the rise of Large Language Models (LLMs), offer a data-driven alternative.

Models like PassGAN [22] and PassGPT [23] can learn probabilistic patterns from leaked datasets and generate passwords that mimic human tendencies more closely than rule-based tools. Our previous work compared GPT-based password models against HashCat and found that while LLMs generate more diverse outputs, they still struggle with high-entropy, human-generated passwords [24, 25] . Nonetheless, the flexibility and realism of LLMs make them valuable for both research and education.

In addition to generation, LLMs are being used for password strength estimation. Traditional strength checkers like `zxcvbn` [26] rely on heuristic rules, entropy, and pattern matching. Newer models incorporate edit distance measures (e.g., Levenshtein distance [27]), neural networks, and

Table 1: Top 3 Most Frequent Passwords by Length [21].

Length	Count	Top 3 Passwords
6	43.6M	123456, 000000, 123123
7	26M	1234567, a123456, welcome
8	189M	12345678, Password, Password
9	153M	123456789, Aa@123456, Admin@123
10	160M	1234567890, qwertyuiop, 987654321
11	115M	12345678910, Welcome@123, qwerty12345
12	92M	admintelecom, Password@123, Pakistan@123

even one-class SVMs, as seen in PassMon [28]. Prompt-based techniques now allow ChatGPT and similar models to evaluate password predictability and security posture [29, 30].

Modern frameworks such as PassTSL [31] integrate password generation and strength analysis within a single system using transformer architectures. These hybrid designs signal a shift toward intelligent, adaptive password security solutions that reflect both user behavior and attacker sophistication.

Despite these advancements, cybersecurity education has yet to fully embrace AI-driven password modeling. Most curricula still focus on traditional threat models and legacy tools, missing the opportunity to introduce students to modern generative techniques. Bridging this gap is essential to prepare learners for current and emerging security landscapes.

Together, this literature highlights the need for instructional experiences that move beyond static datasets and tooling toward student-centered exploration of adversarial behavior, a gap directly addressed by the GenAI-PassLab design described next.

3 Related Work

Research in cybersecurity education has increasingly emphasized experiential learning, gamification, and accessibility. Hands-on approaches have been shown to improve student comprehension and retention. Zeng et al. [32] showed that virtual lab environments that simulate realistic scenarios enhance learning outcomes. SEED Labs [15] and Labtainers [16] are two prominent examples that have shaped cybersecurity pedagogy through modular, containerized exercises.

GenAI-PassLab builds upon this tradition by introducing generative AI models into password security training; an area largely missing from existing hands-on resources. Our work also aligns with curriculum design efforts targeting ABET accreditation [33, 34, 35, 36]. These studies emphasize the importance of integrating modern technologies into computing education to meet evolving workforce needs.

Emerging literature has highlighted the role of LLMs in cybersecurity, from threat detection to

vulnerability analysis [37, 38, 39]. PassGAN [22] was among the first to use Generative adversarial network (GANs) to replicate password distributions, while PassGPT [23] advanced the use of LLMs for syntactically plausible password generation. Our lab adopts similar approaches and exposes students to models trained on real-world datasets like RockYou and HaveIBeenPwned.

Cybersecurity awareness for non-computing students has also gained traction. Turner and Turner [40] successfully introduced password education modules into sociology courses, proving the versatility of these topics. Likewise, situated learning frameworks [41] and capture-the-flag games [42] have increased student motivation and interdisciplinary reach.

Studies on password hygiene consistently show poor practices among users, including reuse, predictable patterns, and weak complexity [43, 44, 45]. Educational tools that simulate attacker models, such as HashCat or zxcvbn, provide empirical grounding for awareness and behavior change [46].

Gamification has proven effective in reinforcing these concepts. Scholefield and Shepherd [47] found that embedding game-like tasks improved engagement and conceptual understanding of password security. While our current GenAI-PassLab does not yet incorporate gamification, its modular and interactive design lends itself naturally to such extensions. We envision future versions of the lab incorporating gamified elements that encourage students to generate, evaluate, and refine passwords using real LLM models.

In summary, while prior work has laid a strong foundation for experiential cybersecurity education, there remains a distinct gap in tools that integrate LLMs into password training. GenAI-PassLab fills this niche with a modular, scalable, and AI-enhanced lab framework that prepares students for a data-driven security landscape.

Together, these efforts motivate instructional experiences that combine hands-on experimentation, modern AI techniques, and ethical reflection—an integration that GenAI-PassLab seeks to provide.

3.1 Hands-On Cybersecurity Education

Hands-on laboratory experiences have long been recognized as essential for effective cybersecurity education, enabling students to engage with adversarial thinking, system behavior, and real-world constraints. Prior work in the SIGCSE community highlights the value of experiential learning through platforms such as SEED Labs and related container-based environments, which provide structured, repeatable exercises for teaching security concepts across a range of topics.

More recent efforts have explored password security education using static datasets or predefined attack models, as well as the use of generative approaches such as PassGAN to study password guessing behavior. While these approaches expose students to important security principles, they typically limit opportunities for students to manipulate model training conditions, compare heuristic and AI-based evaluators, or reflect on the ethical implications of using leaked credential data.

GenAI-PassLab builds on this body of work by combining containerized deployment with

student-facing interaction with a generative language model. The lab extends prior hands-on approaches by allowing students to explore how training data, model configuration, and evaluation strategies influence password generation and vulnerability. In doing so, it emphasizes conceptual understanding of adversarial models and ethical considerations rather than tool-specific mastery, complementing existing cybersecurity laboratory frameworks.

4 GenAI-PassLab Development

The lab activities described in this section are explicitly designed to align with the educational goals outlined in the Introduction, with each task mapping to one or more of the stated objectives.

4.1 GenAI-PassLab Infrastructure

4.1.1 Platform

We utilized the Labtainer [16] platform, developed by the Naval Postgraduate School, to host our labs. Labtainers offer modular laboratory environments accessible to students via a virtual machine. This provides a controlled and consistent setting for various lab activities.

A key advantage of Labtainers is their flexibility, allowing users to create, customize, and easily distribute their own labs. We leveraged this capability by developing our custom lab and making it available to students through a simple download link. To use Labtainers, students first install a virtual machine and download the Labtainers base image.

4.1.2 Process: Creating and Exporting Labs

Lab Creation Our lab development began with selecting our topic. This involved establishing the necessary groundwork, including any required data generation, based on the work by [24]. We then focused on designing the lab activities and identifying the essential libraries and scripts students would need.

Once we had a clear lab outline, we began integrating it into the Labtainer environment. This involved creating a new lab and accessing its Dockerfile. The Dockerfile specifies all required dependencies and packages for the lab.

The base Dockerfile only contains the dependencies for a basic Linux environment. We modified it by adding all necessary libraries and scripts required for the lab. These were hosted in a GitHub repository and cloned into the lab's build. Once we were done editing the Dockerfile we built and tested the lab. The overall lab creation process is illustrated in Figure 5.

Lab Exportation and Distribution After testing the lab, we proceeded to export and distribute it. The first step was creating a Docker Hub repository to store the lab's Dockerfile and creating a GitHub repository to host the primary installation files.

We then executed a series of commands to clean, package, and export the Labtainer images to Docker Hub. Finally, we generated a .tar file, uploaded it to our GitHub repository, and provided students with a direct download link. A detailed breakdown of these steps is available in Section 10 of the Lab Designer Guide [48]. A high-level overview of this exportation process is provided in Figure 6.

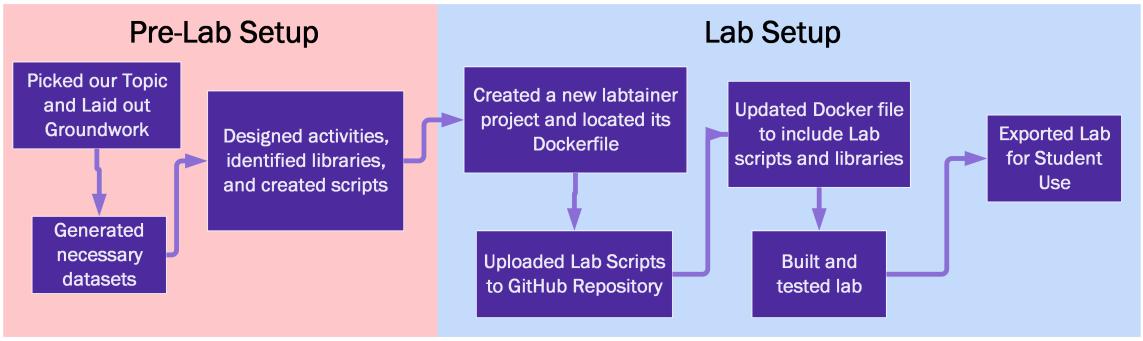


Figure 5: Lab Creation Process

4.1.3 Process: Accessing Our Lab

To access our lab, students obtained a web URL that they used to download the `.tar` archive file, which was available in our GitHub repository. Using this URL, students imported the lab onto their virtual machine. Once students initiated the lab it automatically fetched all of the necessary components and dependencies from the designated Docker Hub repository we set up. After these dependencies were retrieved, students opened and completed the lab. More information on the specifics of this process can be found in Section 10 of the Lab Designer Guide [48].)

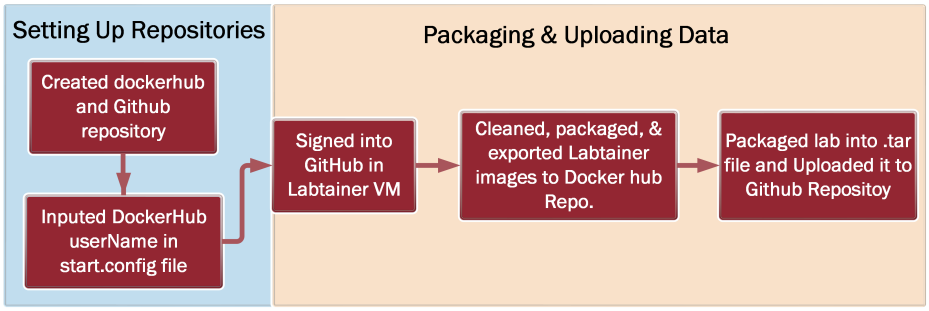


Figure 6: Lab Exportation Process

4.2 LLM-based Password Generation

For this lab, we prepared three GPT-2 models trained using the PassGPT framework [23], each utilizing a different dataset to highlight how training data impacts password generation. The overall process for training and generating passwords is illustrated in Figure 7, which outlines three phases: the Data phase, where a sample password dataset is provided; the Model Training phase, where batches of passwords are fed into the GPT-2 model; and the Password Generation phase, where the trained model outputs new password samples. The PassGPT framework uses a character-level tokenizer, which is better suited for password modeling due to the shorter, keyword-like structure of passwords compared to natural language. This difference in tokenization strategies is illustrated in Figure 8.

Model Selection Rationale GPT-2 was selected for GenAI-PassLab based on pedagogical and practical considerations rather than model performance alone. As a lightweight, open-weight language model, GPT-2 enables students to train, fine-tune, and inspect generative behavior within a controlled environment without reliance on external APIs, usage limits, or variable

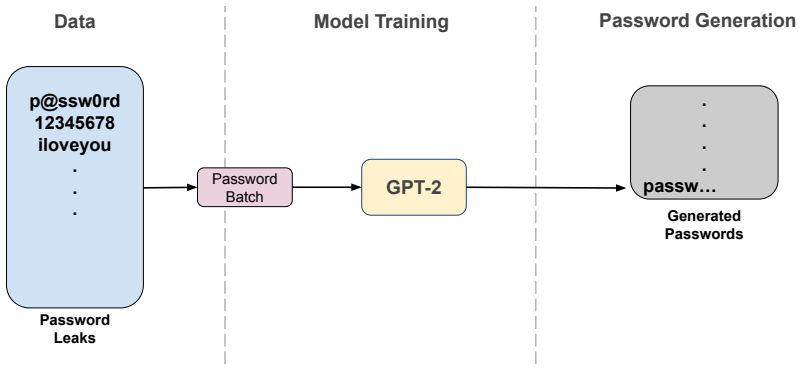


Figure 7: LLM Training and Generation Flowchart

pricing models. This supports reproducibility and allows students to directly observe the effects of training data and parameter choices on model output.

From an instructional perspective, GPT-2 is sufficiently expressive to capture meaningful statistical patterns in real-world password datasets while remaining computationally feasible for classroom deployment. Its relatively small size allows experiments to complete within reasonable time constraints, making it well suited for iterative exploration in a laboratory or homework setting. Importantly, the learning objectives of GenAI-PassLab focus on understanding model behavior, adversarial implications, and ethical considerations rather than on achieving state-of-the-art password generation performance.

While more recent or larger models could be incorporated in future iterations, the use of GPT-2 provides a transparent and accessible platform for teaching core concepts in generative modeling and cybersecurity.

The lab design is model-agnostic, and alternative generative models could be substituted in future offerings without changing the core instructional structure.

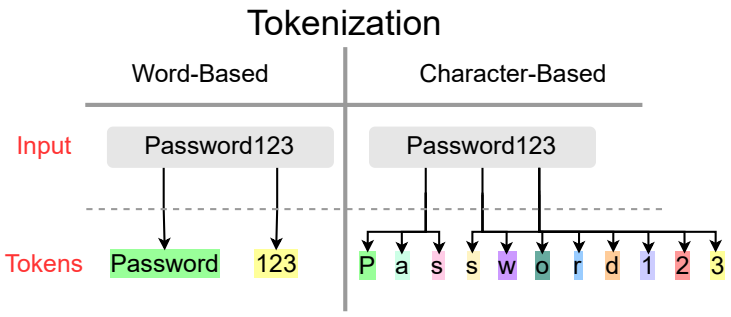


Figure 8: Character-Based vs Word-Based Tokenization

4.3 GenAI-PassLab Overview

The GenAI-PassLab lab gives students interactive exercises covering topics such as password generation using LLMs, password security, and password analysis. The accompanying lab

manual guides students through understanding, generating, and analyzing passwords, and is composed of several sections including a background, pre-lab questions, a walkthrough, and post-lab exercises

4.3.1 Models

The lab provides students with access to three pre-trained password generation models including a model trained on a subset of the *Have I Been Pwned (HIBP)* [49] dataset, a model trained on the *RockYou* [50] dataset and a hybrid model trained on both datasets.

Each model produces password samples with distinct characteristics, allowing students to observe differences in password quality and composition. Additionally, students are given the option to train their own model using a provided password list and the `PassGPT` [23] framework.

4.3.2 Background

This section provides information to help students succeed in later parts of the lab. These include:

- **Password Guessing Models:** A comparison of rule-based and deep learning-based approaches.
- **Dataset Sources:** A discussion of the origins and significance of the HIBP and RockYou datasets.
- **Password Strength Analysis:** An introduction to `zxcvbn`, a password strength estimator that uses pattern matching and real-world cracking techniques to estimate the strength of a password.

4.3.3 Pre-Lab Questions

Students answer a set of questions to assess their understanding of the concepts from the background section. These questions prepare them for the practical activities and exercises. Some example questions include:

- *"What are some real-world datasets commonly used to train password-cracking models, and how were they obtained?"*
- *"How does the password strength estimator zxcvbn evaluate the security of a password?"*

4.3.4 Walkthrough

This section guides students through setting up the environment and generating passwords with pre-trained models. First, students will import the lab files onto their local machine. Next, they will explore the provided scripts and models before using one to generate a set of sample passwords. Finally students will observe and reflect on the characteristics of the passwords they created.

4.3.5 Post-Lab Exercises

The post-lab section includes four key exercises that reinforce the lab's objectives. Each exercise is followed by a series of questions to evaluate student understanding.

1. **Analyzing Passwords Generated Using Different Models:** Students generate 1,000

passwords from two models trained on HIBP and RockYou data and analyze them using `zxcvbn`. They examine password strength, uniqueness, and character type distribution.

2. **Analyzing Passwords Generated with Different Quantities:** Similar to the previous exercise, but students generate 10,000 passwords from each model. They analyze and compare the statistical differences resulting from the increased dataset size.
3. **Analyzing Passwords Using a Merged Data Model:** Students generate passwords using the model trained on both the RockYou and HIBP datasets. They compare the output with the passwords generated from the individual models, analyzing similarities and differences in password quality and strength.
4. **Training and Analyzing Their Own Models:** In this final exercise, students train a custom password generation model using a provided dataset. They then generate and analyze a new set of passwords using the techniques from earlier exercises.

4.4 Student Tasks and Learning Activities

GenAI-PassLab is structured as a sequence of guided, hands-on activities that students complete within a containerized environment. The tasks are designed to support progressive exploration of password security concepts, generative model behavior, and adversarial analysis, while remaining feasible within a standard laboratory session. Each activity produces concrete artifacts that support reflection and discussion.

Task 1: Baseline Password Strength Evaluation. Students begin by analyzing a corpus of passwords using a traditional heuristic-based strength estimator (e.g., `zxcvbn`). They examine password length, entropy estimates, and common structural patterns to establish a baseline understanding of password quality and attacker assumptions.

Task 2: Generative Password Modeling. Students interact with a pre-trained GPT-2 model fine-tuned on leaked password datasets to generate candidate passwords. They observe how the model captures statistical structure in real-world passwords and compare generated outputs to the original dataset.

Task 3: Model Comparison and Training Effects. Students compare password outputs generated under different training conditions (e.g., dataset composition or training duration). This task encourages students to reason about how model training choices influence output diversity, predictability, and security implications.

Task 4: Adversarial Evaluation. Students evaluate AI-generated passwords using both heuristic-based tools and custom scripts, comparing model-based generation against traditional password policies. They analyze which passwords appear strong under heuristics yet remain vulnerable to generative guessing attacks.

Across tasks, students record observations, generate visualizations, and answer guided questions that emphasize interpretation rather than tool mechanics. The sequence is designed to emphasize conceptual understanding of attacker models and system behavior, rather than mastery of a specific AI framework.

Collectively, these tasks are aligned with the educational goals outlined in the Introduction, with

each activity reinforcing student understanding of generative modeling, adversarial reasoning, and ethical considerations in password security.

4.5 Adoption and Availability

GenAI-PassLab was designed with portability and instructional reuse in mind. The lab is implemented using the Labtainers framework and Docker-based containerization, allowing the environment to be deployed consistently across different computing platforms with minimal configuration. All dependencies, model artifacts, and supporting scripts are encapsulated within containers, reducing setup overhead for instructors and students.

The lab is structured as a modular activity that can be integrated into undergraduate or graduate courses in cybersecurity, computer science, or applied machine learning. In its current form, the core activities can be completed within a single laboratory session or assigned as a take-home exercise, with optional extensions for deeper exploration.

At present, the GenAI-PassLab materials are maintained internally to support ongoing refinement. However, documentation describing the lab structure, learning objectives, task sequence, and technical requirements is available to interested educators upon request. We plan to broaden access to the materials in future iterations as licensing and dataset considerations are addressed.

These design choices emphasize reproducibility and ease of adoption, enabling other instructors to focus on pedagogical integration rather than technical setup.

5 Evaluation of GenAI-PassLab

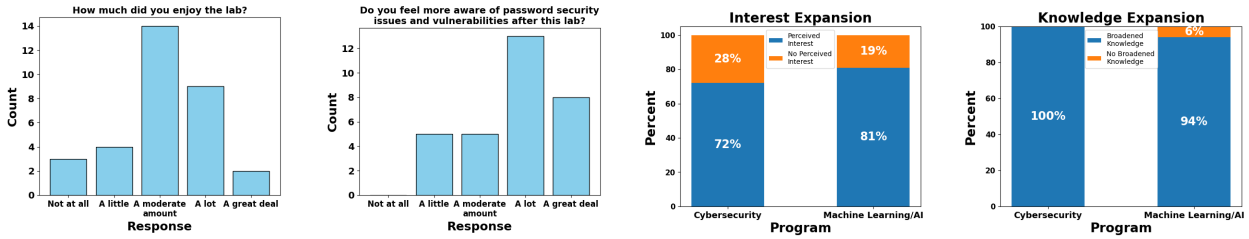
GenAI-PassLab was assigned as a homework activity in computing courses during the Winter 2025 semester. Upon completion of the lab, students were invited to complete an anonymous, voluntary survey designed to capture their perceptions of the learning experience, similar to our prior work on student performance analysis in computing courses [51].

This study was reviewed by the Institutional Review Board (IRB) at our institution and determined to be exempt. Participation in the survey was voluntary, all responses were collected anonymously, and no identifiable student data were retained. All instructional datasets were used solely for educational purposes within a controlled environment, and ethical considerations related to the use of sensitive data were explicitly addressed as part of the lab activities.

The survey was designed to gather feedback on various aspects of the GenAI-PassLab lab and was organized into the following sections:

- **Demographics:** This section collected background information from the students, including their graduate status, year of study, academic major and grade point average (GPA).
- **Learning Comprehension:** This section aimed to assess whether students felt an increased confidence in key subject areas after completing the lab.
- **General Questions:** This part inquired about general aspects of the lab, such as the clarity of instructions and the time taken for completion.

- **Enjoyment, Motivation, and Difficulty Perception:** This section gathered student opinions on their level of enjoyment of the lab, their perception of the lab's difficulty and their level of motivation to participate in completing the lab.
- **Lab Environment and Technical Understanding:** This section focused on the usability of the lab, including the method students used to set up their virtual machine, the ease of setting up the lab environment and the ease of navigating the lab interface.
- **Learning and Interest Expansion:** This part sought to determine. If students learned new concepts from the lab and if the lab heightened their interest in the subject matter including cybersecurity and AI.
- **Suggestions:** This section provided an open-ended opportunity for students to offer any suggestions for improvement regarding the lab.



(a) Enjoyment Ratings (b) Awareness of Security Issues (c) Interest Expansion (d) Knowledge Expansion

Figure 9: Student Feedback Regarding the GenAI-PassLab.

6 Survey Findings

The responses consisted primarily of upper-level undergraduate students, with a majority identifying as juniors or seniors.

The evaluation presented in this section is based on post-lab student survey responses and reflects self-reported perceptions of engagement, confidence, and understanding. The study does not attempt to measure objective learning gains or compare performance against a control group.

The survey results show that students had a positive experience. The majority of students indicated they enjoyed the lab (Figure 9a), suggesting that the hands-on, interactive format was an effective learning method. However, this enjoyment did not come at the expense of challenge. On a 5-point scale where 1 was "Least Difficult" and 5 was "Most Difficult," the lab received an average difficulty rating of 2.77. This indicates the lab successfully struck a balance. It was challenging enough to be stimulating and to require critical thinking, but not so difficult as to be frustrating or demoralizing. Students confirmed that this challenge stemmed from the lab's core activities and problem-solving tasks, not from unclear instructions or technical setup issues. The average completion time of 3.5 hours which we believe is a good amount of time to spend completing this lab.

The data shows a remarkable impact on knowledge acquisition. Every single respondent (100%) reported that the lab broadened their knowledge in cybersecurity, while 94% reported that it

broadened their knowledge in Artificial Intelligence (Figure 9d). This knowledge gain was not merely theoretical. When asked about practical application, most students reported feeling ”a lot” or ”a great deal” more aware of real-world password security issues and vulnerabilities after completing the lab (Figure 9b).

The lab was also a powerful tool for fostering student interest and engagement. A significant majority of students, 72%, indicated that the lab heightened their interest in cybersecurity, while even more (81%) reported an increased interest in AI (Figure 9c).

In conclusion, the survey data confirms that the GenAI-PassLab lab is a well-designed and highly successful educational tool. It provides an enjoyable and engaging experience that is challenging for its target audience. Most importantly, it demonstrably achieves its core learning objectives by significantly expanding student knowledge of both cybersecurity and AI, enhancing their awareness of practical security issues, and effectively stimulating their interest in these fields.

7 Conclusion

The rapid advancements in Artificial Intelligence (AI), Data Science (DS), and Machine Learning (ML) are reshaping both the cybersecurity threat landscape and the tools available to address it. Despite growing interest in AI-powered solutions for offensive and defensive security, educational integration of these technologies remains limited. In particular, the intersection of password security and generative AI offers a compelling but underexplored opportunity for cybersecurity instruction.

This paper introduced **GenAI-PassLab**, an extensible, modular, and research-driven lab designed to bridge this gap. Building on real-world data breaches, large-scale leaked password datasets, and the growing capabilities of Large Language Models (LLMs), GenAI-PassLab equips students with practical skills in password analysis, generation, and strength evaluation. To the best of our knowledge, it is the first hands-on lab focused specifically on password generation using LLMs in a pedagogically structured format.

Our work demonstrates how recent research outputs, including models like PassGPT and our prior work [24], can be transformed into hands-on educational material. By combining classical tools such as HashCat and zxcvbn with modern LLM-based techniques, GenAI-PassLab allows students to explore attacker models, assess password robustness, and reflect on ethical considerations related to leaked datasets.

Furthermore, the lab aligns with key curricular frameworks such as ABET criteria, ACM CSEC 2017 Knowledge Areas, and NIST NICE competencies, and is deployable across computing and non-computing courses alike. Classroom deployments indicated high levels of student engagement and positive self-reported perceptions of learning related to AI-based password security.

Looking forward, we aim to extend this work as part of a broader **AMD4CYB** (AI/DS/ML for Cybersecurity) initiative, in which we convert our own peer-reviewed cybersecurity research papers [52, 53, 54, 55] into experiential, self-contained labs. These labs will cover diverse topics such as such as AI-driven intrusion detection [56, 57], machine learning for cyber-physical systems [53, 54], and time-series modeling for threat detection [52]. The **GenAI-PassLab**

materials are currently available to educators upon request and are planned for broader public release through the NSF-supported National AI Research Resource (NAIRR), ensuring long-term accessibility and community-wide adoptability.

By lowering the barrier between research innovation and classroom implementation, our approach enables scalable, accessible, and future-facing cybersecurity education—essential for building the next generation of practitioners and researchers in an AI-transformed digital world. While the survey results provide encouraging insight into student perceptions, future work will focus on incorporating objective learning measures and comparative assessments.

Acknowledgment
This material is based upon work supported in part by the National Science Foundation (NSF) under Award No. 2515085 and through access to the Jetstream2 [58, 59] cloud computing platform under the National Artificial Intelligence Research Resource (NAIRR) program. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. The authors gratefully acknowledge the provided computational resources and support.

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, "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/

[7] "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

[8] "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

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

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

[12] 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/

[13] Alexandra Borgeaud, "Value of the AI cybersecurity market worldwide 2023-2030," 2024. [Online]. Available: https://www.statista.com/statistics/1450963/global-ai-cybersecurity-market-size/

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

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

[17] Tyler E Judd, H. Bisgin, Mohammad Derani, Alvin Huseinović, and S. Uludag, "Coalescing research into modular and safe educational cybersecurity labs with AI solutions," in *2024 IEEE Frontiers in Education Conference (FIE) (FIE 2024)*, Washington, USA, Oct. 2024, p. 9.

[18] T. Brewster, "Gambling darling paysafe confirms 7.8 million customers hit in epic old hacks," *Forbes*, 30 Nov. 2015, 2015. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2015/11/30/paysafe-optimal-neteller-moneybookers-gambling-cyberattacks-data-breach/

[19] N. Johnston, "Posts tagged "statistics"," https://njohnston.ca/tag/statistics/, —, accessed: 2025-07-02.

[20] G. A. P. Rodrigues, P. A. G. Fernandes, A. L. M. Serrano, G. P. R. Filho, G. F. Vergara, G. D. Bispo, R. d. O. Albuquerque, and V. P. Gonçalves, "From rockyou to rockyou2024: Analyzing password patterns across generations, their use in industrial systems and vulnerability to password guessing attacks," *Journal of Internet Services and Applications*, vol. 16, no. 1, pp. 69–86, 2025. [Online]. Available: https://journals-sol.sbc.org.br/index.php/jisa/article/view/5034/3172

[21] Specops Software, "Specops 2025 Breached Password Report: Analyzing a Year's Worth of Malware-Stolen Credentials," https://specopssoft.com, 2025, accessed: 2025-07-02.

[22] B. Hitaj, P. Gasti, G. Ateniese, and F. Perez-Cruz, "Passgan: A deep learning approach for password guessing," in *Applied Cryptography and Network Security: 17th International*

Conference, ACNS 2019, Bogota, Colombia, June 5–7, 2019, Proceedings 17. Springer, 2019, pp. 217–237.

[23] J. Rando, F. Perez-Cruz, and B. Hitaj, "Passgpt: Password modeling and (guided) generation with large language models," in *European Symposium on Research in Computer Security*. Springer, 2023, pp. 164–183.

[24] O. Kagnici, H. Bisgin, and S. Uludag, "Evaluating the efficacy of gpt-based password generation on real world data," in *Proceedings of the 1st IEEE Conference on Secure and Trustworthy CyberInfrastructure for IoT and Microelectronics (SaTC-IoTME)*. Dayton, OH, USA: IEEE, February 25–27 2025.

[25] Oguz Kagnici, H. Bisgin, and S. Uludag, "A comparative study of large language models for human-like password generation and predictability," in *2025 IEEE CSNet 9th Cyber Security in Networking Conference*, November 2025.

[26] D. L. Wheeler, "zxcvbn: Low-Budget password strength estimation," in *USENIX*, Austin, TX, Aug. 2016, pp. 157–173.

[27] V. I. Levenshtein, "Binary Codes Capable of Correcting Deletions, Insertions and Reversals," *Soviet Physics Doklady*, vol. 10, p. 707, Feb. 1966.

[28] S. Murmu, H. Kasyap, and S. Tripathy, "Passmon: a technique for password generation and strength estimation," *Journal of Network and Systems Management*, vol. 30, pp. 1–23, 2022.

[29] S. J. Kim and B. M. Lee, "A novel approach to password strength evaluation using chatgpt-based prompt metrics," *IEEE Access*, vol. 12, pp. 175 071–175 080, 2024.

[30] M. Atzori, E. Calò, L. Caruccio, S. Cirillo, G. Polese, and G. Solimando, "Evaluating password strength based on information spread on social networks: A combined approach relying on data reconstruction and generative models," *Online Social Networks and Media*, vol. 42, p. 100278, 2024.

[31] H. Li, Y. Wang, W. Qiu, S. Li, and P. Tang, "Passtsl: Modeling human-created passwords through two-stage learning," in *Aust. Conf on Info Sec & Priv*, 2024, pp. 404–423.

[32] Z. Zeng, Y. Deng, I. Hsiao, D. Huang, and C.-J. Chung, "Improving student learning performance in a virtual hands-on lab system in cybersecurity education," in *2018 IEEE Frontiers in Education Conference (FIE)*, 2018, pp. 1–5.

[33] R. Greenlaw and R. K. Raj, "Abet's cybersecurity accreditation: history, accreditation criteria, and status," *ACM Inroads*, vol. 13, no. 4, pp. 14–21, 2022.

[34] A. M. Almuhaideb and S. Saeed, "A process-based approach to abet accreditation: a case study of a cybersecurity and digital forensics program," *Journal of Information Systems Education*, vol. 32, no. 2, pp. 119–133, 2021.

[35] X. Yue, B. Copus, and H. Park, "How to secure abet accreditation for a cybersecurity program: a case study," *Journal of Computing Sciences in Colleges*, vol. 37, no. 6, pp. 15–24, 2022.

[36] S. W. Turner, Tyler E Judd, and S. Uludag, "Experience implementing an automated assessment system for accreditation," in *2024 IEEE Frontiers in Education Conference (FIE) (FIE 2024)*, Washington, USA, Oct. 2024, p. 9.

[37] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, and K.-K. R. Choo, "Artificial intelligence in cyber security: research advances, challenges, and opportunities," *Artificial Intelligence Review*, vol. 55, no. 2, pp. 1029–1053, Feb 2022. [Online]. Available: https://doi.org/10.1007/s10462-021-09976-0

[38] H. Xu, S. Wang, N. Li, K. Wang, Y. Zhao, K. Chen, T. Yu, Y. Liu, and H. Wang, "Large language models for cyber security: A systematic literature review," 2024. [Online]. Available: https://arxiv.org/abs/2405.04760

[39] I. Hasanov, S. Virtanen, A. Hakkala, and J. Isoaho, "Application of large language models in cybersecurity: A systematic literature review," *IEEE Access*, vol. 12, pp. 176 751–176 778, 2024.

[40] C. Turner and C. Turner, "Integrating cybersecurity into the sociology curriculum: the case of the password module," *Journal of Computing Sciences in Colleges*, vol. 33, no. 1, pp. 109–117, 2017.

[41] A. R. Pratama, M. Alshaikh, and T. Alharbi, "Increasing cybersecurity awareness through situated e-learning: a survey experiment," in *The 2nd Global Trends in E-Learning Forum (GTEL 2023)*, 2023.

[42] K. Leune and S. J. Petrilli Jr, "Using capture-the-flag to enhance the effectiveness of cybersecurity education," in *Proceedings of the 18th annual conference on information technology education*, 2017, pp. 47–52.

[43] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor, "" i added'!'at the end to make it secure": Observing password creation in the lab," in *Eleventh symposium on usable privacy and security (SOUPS 2015)*, 2015, pp. 123–140.

[44] V. Taneski, M. Heričko, and B. Brumen, "Impact of security education on password change," in *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2015, pp. 1350–1355.

[45] M. Awad, Z. Al-Qudah, S. Idwan, and A. H. Jallad, "Password security: Password behavior analysis at a small university," in *2016 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA)*, 2016, pp. 1–4.

[46] P. Tsokkis and E. Stavrou, "A password generator tool to increase users' awareness on bad password construction strategies," in *2018 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2018, pp. 1–5.

[47] S. Scholefield and L. A. Shepherd, "Gamification techniques for raising cyber security awareness," in *First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference*. Springer, 2019, pp. 191–203.

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

[49] T. Hunt, “Have i been pwned,” 2013. [Online]. Available: https://haveibeenpwned.com/

[50] R. Mutalik, D. Chheda, Z. Shaikh, and D. Toradmalle, “Rockyou,” 2021. [Online]. Available: https://dx.doi.org/10.21227/gzcg-yc14

[51] H. Bisgin, M. Mani, and S. Uludag, “Delineating factors that influence student performance in a data structures course,” in *2018 IEEE Frontiers in Education Conference (FIE)*, Oct 2018, pp. 1–9. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8659300

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

[53] 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.

[54] 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.

[55] Huseinovic, Alvin, H. Bisgin, Y. Korkmaz, and S. Uludag, “Using Deep Learning Approach to Detect Mixed-rate Data Spoofing in PMUs,” in *2025 33rd IEEE Telecommunication Forum (TELFOR)*, Belgrade, Serbia, Nov 2025.

[56] Onur Sahin and S. Uludag, “Leveraging inter-arrival time for efficient threat filtering: A parsimonious approach,” *Computers & Security*, vol. 154, p. 104471, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404825001609

[57] Doshi, Keval, Y. Yilmaz, and S. Uludag, “Timely Detection and Mitigation of Stealthy DDoS Attacks Via IoT Networks,” *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2164–2176, Sep-Oct 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9316792/

[58] D. Y. Hancock, J. Fischer, J. M. Lowe, W. Snapp-Childs, M. Pierce, S. Marru, J. E. Coulter, M. Vaughn, B. Beck, N. Merchant, E. Skidmore, and G. Jacobs, “Jetstream2: Accelerating cloud computing via jetstream,” in *Practice and Experience in Advanced Research Computing (PEARC ’21)*. New York, NY, USA: Association for Computing Machinery, 2021.

[59] T. J. Boerner, S. Deems, T. R. Furlani, S. L. Knuth, and J. Towns, “ACCESS: Advancing innovation: NSF’s advanced cyberinfrastructure coordination ecosystem: Services & support,” in *Practice and Experience in Advanced Research Computing (PEARC ’23)*. New York, NY, USA: Association for Computing Machinery, 2023.