CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 5, No. 2
October 2026
ISSN: 2832-1006

In this issue:

iscap
Information Systems & Computing Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

2026 Review Board

Bridging the Cybersecurity Skills Gap by Leveraging Cybersecurity Clinics: Developing the Arizona Cybersecurity Clinic

Paul Wagner
paulewagner@arizona.edu

Robert Honomichl
rjhonomichl@arizona.edu

Shengjie Xu
sjxu@arizona.edu

University of Arizona
Tucson, AZ, 85721, USA

Abstract

As cybersecurity threats increase in frequency and sophistication, a widening gap is emerging between the theoretical knowledge offered by academic programs and the practical skills demanded by industry. Experiential learning has emerged as a critical pedagogical approach to bridge this gap by enabling students to apply classroom knowledge to real-world challenges. This paper explores the development of the Arizona Cybersecurity Clinic at the University of Arizona; a program offers hands-on cybersecurity training to students while providing essential services to underserved and under-resourced organizations throughout the state. Drawing inspiration from existing clinic models and leveraging partnerships with secondary and postsecondary institutions, the clinic integrates capstone coursework, micro-credentials, and community engagement to enhance student readiness and regional cyber resilience. The paper details clinic design decisions, curriculum structure, legal and operational documentation, recruitment strategies, and initial implementation outcomes. Notably, the clinic's partnership with Chandler Unified School District marks the first high school-based cybersecurity clinic in the nation, expanding access and pathways into the cybersecurity workforce. Early results suggest that the clinic model effectively supports workforce development, strengthens local cybersecurity postures, and fosters inclusive education through interdisciplinary and intergenerational collaboration. The paper concludes by outlining future directions, including statewide clinic expansion, the development of AI-enhanced capabilities, and efforts to secure sustainable funding. The Arizona Cybersecurity Clinic offers a replicable model for institutions seeking to combine education, service, and innovation in response to the nation's cybersecurity workforce and resilience challenges.

Keywords: Cybersecurity, Cybersecurity Education, Cybersecurity Clinics, Skills Gap, Experiential Learning

Recommended Citation: Wagner, P., Honomichl, R., Xu, S., (2026). Bridging the Cybersecurity Skills Gap by Leveraging Cybersecurity Clinics: Developing the Arizona Cybersecurity Clinic *Cybersecurity Pedagogy and Practice Journal;* v5(n2) pp 4-33. DOI# https://doi.org/10.62273/VMFM4206

Bridging the Cybersecurity Skills Gap by Leveraging Cybersecurity Clinics: Developing the Arizona Cybersecurity Clinic

Paul Wagner, Robert Honomichl and Shengjie Xu

1. INTRODUCTION

Cybersecurity threats are evolving their capabilities at an exponential rate, with industry and educational institutions struggling to keep up. Traditional educational methods often leave a significant gap in practical experience among graduates. Cybersecurity education often emphasizes theory over practice. While theoretical knowledge forms the foundation of cybersecurity education, the lack of hands-on experience limits students' ability to address real-world challenges. Students frequently lack opportunities to apply concepts practically, resulting in a workforce underprepared to tackle dynamic cybersecurity threats and organizational needs. Additionally, employers are increasingly dissatisfied with the ability of recent graduates to perform the required tasks for their job roles.

Experiential learning is a pedagogical approach emphasizing learning through action and application. In cybersecurity, it allows students to engage in simulated environments, hands-on labs, and real-world projects. Experiential learning bridges the gap between theory and practice, developing critical thinking, problem solving, and technical proficiency. Traditional options for experiential learning include labs, simulations, Capture the Flag (CTF) events, bootcamps, workshops, internships, and case studies. This paper will review the literature to understand the current state of the cybersecurity workforce, define experiential learning, and provide an overview of the development and expansion of cybersecurity clinics in the U.S. This paper will then review the development of the Arizona Cybersecurity Clinic, challenges, and initial outcomes. Finally, future work will be discussed, outlining several key initiatives.

2. LITERATURE REVIEW

The rapid global digitization of society, coupled with the increasing sophistication of cybersecurity threats, requires a competent and qualified cybersecurity workforce. However, literature increasingly indicates a disconnect between the competencies of recent college graduates in cybersecurity and related fields and the expectations of employers.

Workforce Development

The demand for skilled cybersecurity professionals continues to outpace the supply. According to ISC2's Cybersecurity Workforce Study (International Information System Security Certification Consortium [ISC2], 2023), there are nearly four million unfilled positions globally, and Cyberseek (Cyberseek, 2025) reports over 450,000 unfilled positions in the United States (U.S.). Employers increasingly feel pressure to fill this gap to protect critical infrastructure, sensitive data, and organizational assets. Despite efforts by academic institutions to expand cybersecurity programs, like those designated under the National Security Agency's (NSA) National Centers of Academic Excellence in Cybersecurity (NCAE-C) program (National Security Agency [NSA], 2025), employers report dissatisfaction with the readiness of recent graduates to meet industry demands.

Employers seek candidates with technical, analytical, and problem-solving skills blended with critical written and verbal professional skills to address the evolving challenges of cybersecurity. The study from ISACA (2023) indicates that employers are dissatisfied with recent graduates' lack of the necessary skills and experience in key areas such as hands-on technical proficiency, incident response and threat mitigation, as well as soft skills and effective communication. ISACA (2023) identified that only 26 percent of those surveyed believe that at least half of the applicants are well qualified for positions. Additionally, soft skills were identified as the most significant skills gap among cybersecurity professionals. Furthermore, despite 52 percent of organizations requiring a degree to fill entry-level cybersecurity positions, 72% of survey respondents neither agree nor strongly agree that university graduates are well prepared to meet the cybersecurity challenges within their organization (ISACA, 2023).

Experiential Learning

ISACA (2023) identified that prior hands-on cybersecurity experience was very important (72%) or somewhat important (23%), and hands-on training was very important (25%) or somewhat important (55%). Individuals entering

into the cybersecurity field and undergraduate students face challenges in acquiring the experience and hands-on training that are important to employers. Experiential learning provides an opportunity to integrate experience and hands-on training into formal education programs.

Experiential learning has been defined in multiple ways; however, most emphasize direct engagement rather than passive study (Houle, 1980; Smith, 2010; Kolb, 2015). Learners can enter the learning cycle at any point; however, all stages in the cycle must be addressed for meaningful learning to occur (Brock University, 2025).

Cybersecurity Clinics

Cybersecurity clinics are modeled after the clinic models found in law and medical schools. Cybersecurity clinics are typically housed and operated out of colleges and universities under the direction of faculty. Students within these colleges and universities train to provide free cybersecurity assistance to underserved and under-resourced community organizations like small businesses, nonprofits, cities and towns, school districts, and utility companies. Clinics provide skills-based experiential learning opportunities to develop the necessary knowledge, skills, and abilities to become a more effective cybersecurity professionals.

Several universities established security clinics providing the basis for a clinic program. The University of California (UC), Berkeley established a clinic in 2018 focusing on defending nonprofits at risk of politically motivated cyber-attacks (Berkeley Center for Long-Term Cybersecurity, 2025). Berkeley's clinic trains the next generation of digital security leaders, defending the social sector and growing the public-interest technology community (Berkeley Center for Long-Term Cybersecurity, 2025). In 2019, Indiana University (IU) and Massachusetts Institute of Technology (MIT) launched their clinics (The Consortium of Cybersecurity Clinics, 2025). IU's clinic model focuses on improving local and state cyber hygiene. The clinic is "the first of its kind to strive to enhance the critical infrastructure sector of under-resourced stakeholders focusing on local municipalities, counties, school corporations and small businesses (Indiana University, 2025)." MIT's cybersecurity clinic is open to registered students from MIT, Harvard, or Wellesley (Massachusetts Institute of Technology [MIT], 2025). The MIT clinic works with public agencies and urban infrastructures utilizing an approach called Defensive Social Engineering (DSE) and technical tools to defend against cyber-attacks (MIT, 2025).

UC Berkeley, IU, and MIT partnered with the University of Alabama in 2021 to form the Consortium of Cybersecurity Clinics. As of 2025, the Consortium consists of 34 active clinics and five allies (The Consortium of Cybersecurity Clinics, 2025). The Consortium aims to serve as a platform for faculty, students, trainers, and advocates to network and share knowledge, expand the reach of cybersecurity clinics, and lower the barriers for other higher education institutions to establish their own clinics. The overarching vision is to launch a university, college, or community-college based clinic in all 50 U.S. states by 2030 (The Consortium of Cybersecurity Clinics, 2025).

3. CLINIC DEVELOPMENT

Background

The University of Arizona (U of A) was one of 15 institutions awarded a grant to establish the Arizona Cybersecurity Clinic in June 2024, with a period of performance through 2031. U of A clinic personnel envisioned the clinic as a model for the entire state, developing affiliate clinics in collaboration with community colleges, universities, and other partners throughout the state. The Clinic's mission is to create unique and impactful student experiential learning opportunities by providing vital cybersecurity services to underserved under-resourced, and underrepresented organizations throughout Arizona. Its vision is to secure and empower underserved, under-resourced, and underrepresented organizations throughout Arizona by providing cybersecurity awareness training, risk and vulnerability assessments, and other services as needed while cultivating the next generation of cybersecurity leaders.

Prior to developing the clinic, faculty members met with clinic personnel from the University of Nevada Las Vegas (UNLV) (University of Nevada, Las Vegas [UNLV], 2025), Metro State University (Metro State University, 2025), Massachusetts Institute of Technology (MIT) (MIT, 2025), and the Louisiana State University (LSU) (Louisiana State University [LSU], 2025) to learn more about various clinic models. These institutions were selected due to the maturity of their programs, engagement with clinic directors at the Consortium of Cybersecurity Clinics welcome event hosted in June 2024 at the NICE Conference, and their partnerships in the NSA Centers of Academic Excellence in Cybersecurity (NCAE-C) community. Additionally, faculty

reviewed all documents and curriculum shared by existing clinics through the Consortium of Cybersecurity Clinics. Finally, faculty attended monthly Consortium of Cybersecurity Clinics meetings to learn about best practices and initiatives. Based on this analysis, the faculty determined there were three options for operating a cybersecurity clinic: through coursework (capstone, internship, or independent study), through a campus club, or as a paid opportunity. Table 1 outlines the pros and cons of each approach.

It was determined that the capstone model would be the best option for the initial pilot based on this analysis. The course capstone is typically the last course in the student's undergraduate academic journey. Students would have taken most of their program requirements prior to participating in the clinic, providing a solid foundation in cybersecurity concepts. The clinic capstone course has a capacity of 30 students per semester.

Model	Pros	Cons
Coursework	• Students already required to take the course. • Leverages existing student support structures (Advising, Faculty, Staff). • Builds on previous courses and learning.	• Only offered twice per year (Spring / Fall Semester). • Increases student workload. • Student participation limited to junior or senior years.
Campus Club/Unpaid Opportunities	• Option for students to engage earlier in academic journey. • Long-term experiential learning potential. • Not constrained by academic semesters.	• Student led, extra-curricular activity. • May lack experience necessary to develop and maintain the clinic. • Clinic may not be priority for participants. • Limited resources.
Paid Opportunity	• Option for students to engage earlier in academic journey. • Long-term experiential learning potential. • Not constrained by academic semesters. • Prioritizes clinic work.	• High operational costs.

Table 1 – Clinic Model Analysis

Curriculum

The curriculum was developed based on a review of existing curriculum, identifying gaps in the cybersecurity program, the ability to provide clinic opportunities to students not in the cybersecurity program, and the needs of the clients. Clinic personnel evaluated the Cybersecurity Maturity Model Certification (CMMC), NIST Risk Management Framework and Cybersecurity Framework, and the Center for Internet Security (CIS) Critical Security Controls Version 8.1. Based on that evaluation and input from the Consortium of Cybersecurity Clinic members, the CIS controls were selected as the assessment framework. The CIS Controls provdie a broad based adaptable cybersecurity framework that can be applied to organizations of any size or sector. Additionally, CIS provides extensive materials and guides to support assessments. The Arizona Cybersecurity Clinic focused on Implementation Group (IG) 1 Essential Cyber Hygiene, which outlines 56 cyber defense safeguards (Stocchetti, 2024). Table 2 outlines the curriculum developed for the Spring 2025 pilot. It is important to note that the capstone course includes additional lectures and resources, covering topics such as conducting academic research and professional development.

Micro-Credential

Micro-credentials, sometimes referred to as digital badges, are specialized courses that teach specific knowledge, skills, and abilities to prepare students for entry-level jobs. Micro-credentials enable institutions the ability to offer modular learning opportunities, problem-oriented and activity-based teaching, and case studies from industry (Eibl, 2024). Additionally, micro-credentials can offer flexible education tailored to individual learners. The U of A defines a micro-credential as, "a small program in a focused area of study," and a digital badge as, "artifacts, much like a diploma awarded to learners upon completion of a micro-credential program" (University of Arizona, 2025).

Module	Topic	Lecture Length
Module 1.1	Risk Overview	47 minutes
Module 1.2	Risk Management	19 minutes
Module 1.3	Threat Modeling	24 minutes
Module 1.4	Controls and Contingency Planning	24 minutes
Module 1.5	Risk Management Framework	14 minutes
Module 1.6	CIS Controls	14 minutes
Module 1 Supplementary	CIS Controls Documentation Review	12 minutes
Module 1 Supplementary	Clinic Legal Documentation	12 minutes
Module 2.1	Risk Assessment Overview	24 minutes
Module 2.2	Risk Assessment Process	27 minutes
Module 2.3	Clinic Risk Assessment	49 minutes
Module 2 Supplementary	Client Intake Form	35 minutes
Module 2 Supplementary	Rules of Engagement and Scoping	10 minutes
Module 3.1	General Research and Analysis	23 minutes
Module 3.2	Industry Research	40 minutes
Module 3.3	Benchmarks	21 minutes
Module 3.4	Vulnerabilities	29 minutes
Module 3 Supplementary	CISA Critical Infrastructure Sectors	10 minutes
Module 3 Supplementary	Hierarchical Cybersecurity Governance Framework	8 minutes
Module 3 Supplementary	Industry Reports Overview	9 minutes
Module 3 Supplementary	CIS Workbench	9 minutes
Module 4.1	Technical Report	49 minutes
Module 4.2	Presentation	29 minutes
Module 4 Supplementary	Technical Report and Presentation	18 minutes
Module 5.1	Vulnerability Assessment Overview	7 minutes
Module 5.2	Information Gathering	16 minutes
Module 5.3	Information Gathering Demo	40 minutes
Module 5.4	Scanning	19 minutes
Module 5.5	Scanning Demo	18 minutes

Table 2 – Risk Assessment Curriculum Modules

The University developed its micro-credential to ensure learners internal to and external to the University could receive a credential. The University's micro-credential will be available to high school, undergraduate, graduate, and continuing and professional education students. The National Association of Colleges and Employers (NACE) identifies eight career readiness competencies: career & self-development, communication, critical thinking, equity & inclusion, leadership, professionalism, teamwork, and technology (National Association of Colleges and Employers [NACE], 2024). The University's badge credentials aligned with career & self-development, critical thinking, professionalism, technology, and leadership competencies.

The minimum amount of time commitment to receive the micro-credential is 40 hours, which is outlined as:

Risk Assessment Modules (5) – 12 hours

- Cyber Risk and Vulnerability Assessment and Document Review – 15 hours
- Research and Analysis – 10 hours
- Report and Presentation Preparation – 12 hours

The minimum amount of time commitment to receive the micro-credential is 40 hours, which is outlined as:

- Risk Assessment Modules (5) – 12 hours
- Cyber Risk and Vulnerability Assessment and Document Review – 15 hours
- Research and Analysis – 10 hours
- Report and Presentation Preparation – 12 hours
- Report and Presentation Delivery – 1 hour

Figure 1 – University of Arizona Micro-Credential

Documentation
Documentation was divided into two primary categories of legal and assessment. Clinic personnel met with the university's Office of General Counsel (OGC) to identify the forms necessary to meet with and provide services to clients. Additionally, agreement documents were established to develop affiliate clinics to expand the clinic model including the Memorandum of Understanding (MOU) Cybersecurity Clinic (affiliate clinics) (Appendix A), Cybersecurity Clinic Client Memorandum of Understanding (MOU) (Appendix B), Student Non-Disclosure Agreement (NDA) (Appendix C), and Student Code of Conduct (Appendix D).

Services
Initially, the clinic would work with clients to provide cybersecurity awareness training, risk assessments, and vulnerability assessments as needed. A series of cybersecurity awareness training presentations were developed to support clients and community organizations. Risk assessments would consist of an initial intake form (Appendix E) and a risk assessment checklist. This process would provide an initial baseline of clients for "Essential Cyber Hygiene." Clients could also request vulnerability assessments consisting of network, web application, and system scans using open source tools like Nmap, Zed Attack Proxy (ZAP), and OpenVAS. Enterprise tools such as Nessus and Burp Suite were evaluated and initially determined to be cost prohibitive. It is important to note that vulnerability assessments introduce risk to the assessment process, as potential students may not be qualified or trained to properly conduct these tests. Additionally, clients may have concerns with students actively engaging with their environment. Further, penetration testing was considered but ultimately would not be implemented until after the initial pilot due to increased risk.

Clinic personnel took several steps to minimize client risk and maximize quality. Data collection, specifically, sensitive data collection was minimized. All data, records, and documentation was hosted on the university's secure cloud platform. Students were provided read only access to any sensitive information to minimize risk of downloading or propagating information. Clinic personnel ran all vulnerability scans and provided the results to students. Additionally, clinic personnel established mock interviews to prepare for presentations and conducted multiple rounds of revisions for the technical report. Further, clinic personnel set up weekly office hours and set up group meetings to answer questions and keep assessments on track to meet deliverable timelines.

Client Recruitment
Initial client recruitment occurred in several ways. Upon receipt of the grant, local outlets published a story about the Arizona Cybersecurity Clinic (Burtch-Buus, 2024; Blaser, 2024). This led to organizations and community groups reaching out to connect, provide presentations, and provide security awareness training. Clinic personnel presented at local, regional, and national events and conferences to discuss the clinic and its services. Finally, partners within Arizona's cybersecurity education ecosystem were asked to participate in the pilot. This resulted in identifying nine clients for the initial pilot. Currently the clinic has capacity to support a maximum of 15 clients per semester.

Student Recruitment
Like client recruitment, clinic personnel recruited students in several ways. A presentation was provided to U of A's cybersecurity club. Although this was intended to recruit students for the Spring 2025 pilot, the perpetual club model was described to determine interest in establishing that model within the club. Additionally, the cybersecurity program manager, advisors, and career and engagement coordinator set up information sessions for students. Thirty slots were allocated in the senior capstone course for the pilot.

Upon completion of this initial outreach, students taking their senior capstone in Spring 2025 were notified of the opportunity to participate in the clinic. Students within the Cyber Operations, Applied Computing, and Intelligence and Information Operations (IIO) programs were included, providing an interdisciplinary approach

to the clinic. It is important to note that students are predominantly online, adult learners. Interested students were required to complete an application expressing their interest, describe their motivation for participating, and complete an agreement form stating they would need to be available to meet with clients during Arizona business hours or as required. This was an important distinction due to the typical asynchronous availability of online students and competing priorities of adult learners. Thirty-three students began the application process, with 31 students completing the application. Of those, 26 students were selected to participate in the Spring 2025 pilot.

Chandler Unified School District (CUSD)

U of A's cybersecurity program has worked closely with Chandler Unified School District's (CUSD) cybersecurity program. CUSD's program is offered through Basha High School's Institute of Cyber Operations and Networking (ICON). It is a Career Technical Education (CTE) program that provides students with up to four years of high school cybersecurity education, up to 30 college credits through their dual enrollment program, and articulated pathways with Chandler Gilbert Community College (CGCC) and U of A. Clinic personnel met with CUSD's cybersecurity director to discuss the possibility of partnering to provide the clinic opportunity to high school students. Presentations were provided to students at three district high schools: Basha High School, Arizona College Preparatory (ACP) High School, and Chandler High School.

Ninety-six students from these high schools began the Google Cybersecurity Certificate course in Fall 2024 to prepare for participation in a pilot clinic in Spring 2025. An agreement between the U of A and CUSD was signed in November 2024, establishing the district as the first affiliate cybersecurity clinic in Arizona and the first high school cybersecurity clinic nationally (Dowd, 2024).

The CUSD Cybersecurity Clinic was initially planned as a two phase program. Students would be enrolled in the Google Cybersecurity Professional Certificate program during the fall term and complete modules and activities for the U of A's micro-credential during the spring term. Students must complete the certificate before continuing with the micro-credential. Participation in the clinic was voluntary, and students were required to complete training and modules after school.

4. INITIAL RESULTS

Initial results for the program were assessed based on student participation, feedback provided from students and clients during After Action Reviews (AAR), Student Course Surveys, and faculty and staff reflections. This section is broken down into the high school cybersecurity clinic and post-secondary cybersecurity clinic pilots which concluded in May 2025. Clinic operations will be evaluated and assessed after each semester to identify additional lessons learned, key performance indicators, and opportunities.

Post-Secondary Cybersecurity Clinic

The Arizona Cybersecurity Clinic concluded the initial pilot program in May 2025. This section outlines the initial results and lessons learned from the pilot. The 26 post-secondary capstone students were initially divided into groups of three to support eight clients. These clients represented municipal governments (2), non-profits (2), small businesses (3), critical infrastructure (1). Although all students completed the training and the capstone course, only seven of the eight groups were able to provide the detailed report and present their findings to the client. The group that didn't complete the report and present the findings was due to timelines, scheduling conflicts, and other issues that couldn't be overcome during the academic semester. Despite the level of work required in the course and the challenges of participating in a pilot course, all students stated that they were glad that they participated in the opportunity and would recommend it to other students. Specific comments from student course surveys include:

"First, the application of concepts learned in the classroom to a real-world experience. Second, it was also challenging on multiple levels such as working independently and as a group, putting together and finalizing a client presentation and technical report, etc. This format allowed for learning multiple new skills."

"I really appreciated that we were able to conduct a "real life" risk assessment for a local company and apply our knowledge in the best and most interactive way possible while in class. This felt like an internship within an academic setting."

"It was a full circle moment, everything I learned in the cyber operations side was brought together, and I got to reflect on my journey here."

Despite the positive feedback from students and clients, there were many lessons learned. All students participated in an After Action Review

(AAR) to identify what went well, areas of improvement, key takeaways, and assess whether the opportunity was worthwhile. Additionally, clinic staff, faculty, and mentors participated in a separate AAR to review the course materials and identify lessons learned. The following are the three major changes that will be implemented for the Fall 2025 cohort:

- Client Contracts: Contract delays shifted the timeline three to four weeks, reducing student-client engagement. Future contracts will be finalized as soon as clients are identified to avoid disruptions.
- Group Assignment: Delays also postponed group formation and team norming. Going forward, groups will be assigned before the semester begins, with required early sessions to establish expectations and communication practices.
- Streamlining Requirements: Students previously completed multiple individual research deliverables that were later synthesized into the client report. In the future, groups will collaborate on these elements from the start, with faculty assessing the effectiveness of this approach.

High School Cybersecurity Clinic (CUSD)

CUSD held the ribbon cutting for their cybersecurity clinic on March 25, 2025. Government representatives; Department of Homeland Security (DHS); administrators, faculty and staff from secondary and post-secondary institutions, and industry and community partners attended the ribbon cutting. The event recognized the 59 students that completed the Google Cybersecurity Professional Certificate. Of the 59 students, 30 students opted to continue with the second phase of the program completing the Cybersecurity Risk and Vulnerability Assessment micro-credential. The primary reason cited by students for not continuing with phase two was the time commitment to meet after school.

Additionally, the district established an internship program for clinic students. Interns will lead study sessions for the Google Cybersecurity Professional Certificate with new clinic participants, develop and present cybersecurity awareness training to community organizations and businesses, attend small business meetings, and maintain a professional journal of outreach activities and reflections. This will further expand these students' professional and technical skills and build their professional network.

5. FUTURE WORK

The development and expansion of the cybersecurity clinics provide several opportunities to support student experiential learning and enhance the cybersecurity of citizens and communities. This section outlines several key initiatives to refine and expand clinic operations.

Clinic Refinement

Lessons learned from the CUSD, and U of A pilots will provide valuable insight into the curriculum, assessment tools, methodologies, and operations. Faculty, staff, students, and clients will be involved in analyzing the clinic model to enhance training while streamlining operations. The deliverable from this assessment is a comprehensive Standard Operating Procedure (SOP) that can be shared with other organizations to establish affiliate clinics in Arizona and support the broader Consortium of Cybersecurity Clinics.

Clinic Expansion

The Arizona Cybersecurity Clinic is partnering with Pima Community College (Tucson, Arizona), Estrella Mountain Community College (Avondale, Arizona), and Grand Canyon University (Phoenix, Arizona) to develop affiliate clinics to support Pima and Maricopa Counties. Faculty at the four institutions are going through professional development training and reviewing curriculum materials in Summer 2025 and a student pilot will begin in Fall 2025.

The U of A will explore a perpetual model like UNLV. The clinic is working with students to develop a plan to promote and support this initiative. Clinic expansion requires considerable resources to operate, both in terms of time and funding. These constraints may be a limiting factor. Additionally, most undergraduate cybersecurity students at U of A are remote, online, adult learners creating opportunities and challenges for developing this model.

Further, clinic operations will be evaluated to determine capacity and expansion within U of A's capstone course. Currently one section of the capstone course is offered each semester with a capacity of 30 students. This can support up to 15 clients with students working in groups of two. Clinic personnel will track the time required to support student groups and client engagement to determine the approximate time per client needed. Although client capacity has not been reached, clinic personnel will develop selection criteria for clients.

Finally, the CUSD model will expand due to interest and demand. The program will be expanded to a two year program. Year 1 will consist of the Google Cybersecurity Professional Certificate (Fall) and the Cybersecurity Risk and Vulnerability Assessment micro-credential (Spring). Students that completed these requirements during Academic Year 2024-2025 will be eligible to participate in the pilot of Year 2. Year 2 will have students apply what they learned and develop professional skills. Students will provide peer mentorship to Year 1 students, develop cybersecurity awareness training modules to support the school district and community organizations, conduct cyber hygiene outreach to the community.

Community Engagement

Community engagement will expand in 2025. This will be achieved directly through client engagement during the pilot and through local, state, and national outreach efforts. Partnerships are critical to meet the goals and of the clinic. The Arizona Cybersecurity Clinic is working with government, non-profit, and industry organizations throughout Arizona to expand opportunities. Faculty and students will attend meetings, events, and conferences to share their experiences and findings. Additionally, the clinic will provide security awareness training to citizens and community organizations. This meets one of the clinic's core missions while generating leads for potential clients and expanding the clinic's footprint. Furthermore, the Clinic is collaborating with universities to develop and host statewide Capture the Flag events, run summer camps, and offer professional development for middle and high school students and teachers to promote cybersecurity awareness and competencies.

Funding

Initial funding supports foundational operations for the Arizona Cybersecurity Clinic. Additional funding is necessary to support student development and expansion of the clinic model throughout Arizona. Students, especially first-generation and minority students, often face the decision between seeking paid employment in unrelated fields or gaining cybersecurity experience through volunteer opportunities. Funding would provide students with the opportunity to obtain paid student worker positions within the clinic, thereby offsetting the need for an "either or" decision. Additionally, certifications are important for gaining employment in the cybersecurity field. The ability to provide students with certification vouchers removes barriers to obtaining these certifications. The clinic is well-positioned to provide training for students across a variety of certifications to support employment in the field. Further, certified students are better equipped to provide clinic services to clients. Finally, the ability for organizations and secondary and postsecondary schools to develop and sustain a clinic requires additional resources. These and other considerations will drive the identification of partnerships, grants, and donations to support the growth and expansion of opportunities for students.

AI-Driven Tasks

As technology evolves, artificial intelligence (AI) presents a significant opportunity to strengthen the clinic's impact by improving efficiency, scalability, and effectiveness in cybersecurity operations. AI can enhance vulnerability assessments by automating security assessments, analyzing threat intelligence, detecting anomalies, and generating reports. These tools enable continuous monitoring enabling real-time identification of weaknesses in networks, applications, and endpoints, reducing manual effort for students and faculty while improving quality.

AI can also improve cybersecurity awareness training. Adaptive learning platforms can tailor modules to individual knowledge gaps, while simulated phishing attacks identify employees susceptible to social engineering and guide targeted education. AI-powered chatbots can provide real-time guidance and reinforce best practices, while gamification and adaptive methods increase engagement and retention.

The clinic will further pursue research at the intersection of AI and cybersecurity. Priorities include ethical AI, bias mitigation, and explainable AI to ensure transparency and trust in automated decisions. Collaborations with industry and academia will also explore AI-powered threat intelligence sharing to advance real-time information exchange and collective defense.

6. CONCLUSIONS

The development of the Arizona Cybersecurity Clinic represents a strategic and timely response to the growing demand for experiential learning in cybersecurity education. By bridging the gap between academic theory and real-world practice, the clinic offers a model that not only enhances student readiness for the workforce but also provides vital cybersecurity support to underserved and under-resourced organizations. This case study demonstrates the potential of cybersecurity clinics to address workforce

shortages, elevate community cyber hygiene, and promote interdisciplinary collaboration across educational levels.

The initial pilot at the University of Arizona, along with its partnership with Chandler Unified School District, illustrates the feasibility and scalability of a clinic-based experiential learning model. Key achievements include a well-structured curriculum, effective student and client recruitment strategies, and the development of supporting legal and educational documentation. Importantly, the implementation of micro-credentials further supports flexible and inclusive access to cybersecurity education for learners across a broad spectrum.

The clinic's expansion through affiliate partnerships, AI-enhanced capabilities, and increased community engagement promises to deepen its impact. Sustained funding and strategic collaborations will be essential to ensure the model's long-term success and replicability. As cybersecurity threats continue to evolve, so too must our educational models. The Arizona Cybersecurity Clinic offers a compelling blueprint for how institutions can lead in this critical domain by combining pedagogy, public service, and innovation.

7. REFERENCES

About the Consortium. (2025). *About the consortium: History of the consortium*. The Consortium of Cybersecurity Clinics. https://cybersecurityclinics.org/about/

Berkeley. (2025). *UC Berkeley cybersecurity clinic*. Berkeley Center for Long-Term Cybersecurity. https://cltc.berkeley.edu/program/cybersecurity-clinic/

Blaser, S. (2024, June 13). *University of Arizona gets $1M from Google for new cybersecurity clinic*. *Arizona Daily Star.* https://tucson.com/news/local/business/university-of-arizona-cybersecurity-google-business/article_38751718-2909-11ef-aa25-bb580e88046d.html

Burtch-Buus, L. (2024, June 12). *Cybersecurity clinic will protect businesses from online threats, develop students' career skills*. *University of Arizona News.* https://news.arizona.edu/news/cybersecurity-clinic-will-protect-businesses-online-threats-develop-students-career-skills

Brock University. (2025). *Pedagogy of experiential education*. Centre for Pedagogical Innovation, Brock University. https://brocku.ca/pedagogical-innovation/resources/experiential-education/pedagogy-of-experiential-education/

Cyber Clinic. (2025). *UNLV Cyber Clinic*. Office of Economic Development, University of Nevada, Las Vegas. https://www.unlv.edu/econdev/cyber-clinic

Cybersecurity for the public good. (2025). *Welcome to the consortium: Cybersecurity for the public good*. The Consortium of Cybersecurity Clinics. https://cybersecurityclinics.org/

Cyberseek. (2025). *Cyberseek supply and demand heat map*. https://www.cyberseek.org/heatmap.html

Dowd, B. (2024, November 1). *Chandler district partners with UA to expand high school cybersecurity program*. *KJZZ Phoenix.* https://www.kjzz.org/education/2024-11-01/chandler-district-partners-with-ua-to-expand-high-school-cybersecurity-program

Eibl, G., Jungbauer, D., Litvyak, O., Luidold, C., & Völkl, P. (2024, September 13). *Proactive curriculum development for cybersecurity education: A model of micro-credentials and active blended learning*. *ACM.* https://doi.org/10.1145/3670243.3673882

Houle, C. (1980). *Continuing learning in the professions*. Jossey-Bass.

Indiana University. (2025). *A global challenge, a local priority: Indiana University cybersecurity clinic*. IU Cybersecurity Clinic. https://cyberrisk.iu.edu/career-prep/cyberclinic.html

International Information System Security Certification Consortium (ISC2). (2023). *How the economy, skills gap, and artificial intelligence are challenging the global cybersecurity workforce*. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e

ISACA. (2023). *State of cybersecurity 2023: Global update on workforce efforts, resources, and cyberoperations*. https://www.isaca.org/state-of-cybersecurity-2023?utm_source=other&utm_medium=other&utm_campaign=pr_both_content_survey-report_state-of-cybersecurity-survey-2023_quarter-3-2023_state-of-cybersecurity-2023-press-release&utm_content=state-of-cybersecurity-survey-2023_state-of-cybersecurity-2023-press-release&cid=pr_3000043&Appeal=pr

Kolb, D. A. (2015). *Experiential learning: Experience as the source of learning and development*. Pearson Education. https://www.cisecurity.org/insights/white-papers/guide-implementation-groups-ig-cis-critical-security-controls-v8-1

Kolb, D. A. (2025). *What is experiential learning*. Institute for Experiential Learning. https://experientiallearninginstitute.org/what-is-experiential-learning/

Louisiana State University. (2025). *LSU cybersecurity clinic*. https://www.lsu.edu/cyberclinic/index.php

Massachusetts Institute of Technology. (2025). *Cybersecurity: A social engineering approach at MIT*. https://urbancyberdefense.mit.edu/cybersecurityclinic/

Metro State University. (2025). *MN Cyber Clinic*. https://www.metrostate.edu/mncyber/clinic

National Association of Colleges and Employers. (2024). *Competencies for a career-ready workforce*. https://www.naceweb.org/docs/default-source/default-document-library/2024/resources/nace-career-readiness-competencies-revised-apr-2024.pdf?sfvrsn=1e695024_6

National Security Agency. (2025). *National Centers of Academic Excellence in Cybersecurity (NCAE-C).* https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

Smith, M. (2010). *David A. Kolb on experiential learning*. The encyclopedia of pedagogy and informal education. https://infed.org/mobi/david-a-kolb-on-experiential-learning/

Stocchetti, V., Franklin, J., & Regnier, R. (2024, November). *Guide to implementation groups (IG) CIS critical security controls v8.1*. Center for Internet Security. https://www.cisecurity.org/insights/white-papers/guide-implementation-groups-ig-cis-critical-security-controls-v8-1

The Consortium of Cybersecurity Clinics. (2025). *Our member organizations*. https://cybersecurityclinics.org/about/our-members/

University of Arizona. (2025). *Micro-credentials and digital badges*. Office of the Registrar. https://registrar.arizona.edu/badge

APPENDIX A
Memorandum of Understanding Cybersecurity Clinic

MEMORANDUM OF UNDERSTANDING
Cybersecurity Clinic

This Cybersecurity Clinic Memorandum of Understanding (this "Agreement") is effective as of the latest date of signature below (the "Effective Date") between the Arizona Board of Regents, acting for and on behalf of the University of Arizona (the "University") and XXX (the "District").

RECITALS

A. The District is implementing a Cyber Security Academy program (the "Program"), wherein high school students enrolled in schools within the District will have the opportunity to study cybersecurity and to obtain real world experience in the field, such as assessing cybersecurity risks and working collaboratively under instructor supervision to implement cybersecurity policies and technical controls.

B. The University's College of Applied Science and Technology has developed a Cybersecurity Clinic (the "Clinic"), a program similar to the Program for University students.

C. As part of the Clinic, the University has developed and obtained resources and materials that could benefit the Program and enhance the education the District's students receive within the Program.

D. The parties desire to collaborate in order to strengthen both the Program and the Clinic, both in terms of educational benefits for students and for the Arizona community at large, as described in this Agreement.

AGREEMENT

A. **Scope of Collaboration.**

   a. Google Cybersecurity Professional Certificate training ("Google Training")
      i. University will provide the District with training seats for the online Google Training. The number of training seats provided to the District at any given time will depend on both training seat availability and District need.
      ii. District agrees that any training seats provided by the University will be used solely by students enrolled in the Program.

   b. Training and Mentorship
      i. The University will provide training and mentorship to the Program instructors and administrators as reasonably requested.
      ii. The University will also provide Google mentors to the District upon request for the purpose of presenting to Program students.
      iii. The University's ability to provide such Google mentors will depend upon receiving sufficient advanced notice from the District as well as the availability of the Google Mentors.

   c. Materials
      i. The University will provide Clinic materials to the District as reasonably requested for use in the Program. Such materials may include, but are not limited to, risk assessment questionnaires, study materials, and instruction materials.

B. **Compensation.** There will be no compensation provided to or by either party in connection with this Agreement.

C. **No Joint Venture.** It is expressly understood and acknowledged that the parties are entering into this Agreement as independent contractors and that this Agreement is not intended to create,

nor shall it be construed as creating, any type of partnership, joint venture, or franchise relationship between the parties. Each of the parties will direct its own activities pursuant to this Agreement. No party shall have authority to direct the other's activities.

D. **Intellectual Property.**

a. **Ownership.** The parties acknowledge that inventions, discoveries, and other technology that is patentable, or that is copyrightable software ("Intellectual Property") may also arise from the Research Project. University owns all Intellectual Property invented or authored by University personnel under the Research Project ("University Intellectual Property"). The parties will jointly own all Intellectual Property invented or authored jointly by University personnel and Sponsor personnel under the Research Project ("Joint Intellectual Property"). Inventorship and authorship will be determined in accordance with United States intellectual property laws. This Agreement does not grant either party any rights to any Intellectual Property developed outside the scope of the Research Project.

b. **Retained Rights.** Without limiting any other rights it may have, the University specifically reserves the right in and to the University Intellectual Property and Joint Intellectual Property for any research, public service, and/or educational purposes, and to grant licenses to other academic institutions for these same reserved rights.

E. **Arbitration.** The parties agree to arbitrate disputes filed in Arizona Superior Court that are subject to mandatory arbitration pursuant to A.R.S. § 12-133.

F. **Conflict of Interest.** This Agreement is subject to cancellation pursuant to the provisions of A.R.S. § 38-511 regarding Conflict of Interest.

G. **Indemnification.** Neither party to this Agreement agrees to indemnify the other party or hold harmless the other party from liability hereunder. However, each party will be responsible for any and all liability caused by the act, omission, negligence, misconduct, or other fault of their employees, agents, and officers arising from this Agreement.

H. **Insurance.** The parties recognize that the Arizona Board of Regents participates in the Arizona State Risk Management Program. Any liability of the State of Arizona resulting from any negligence of its employees shall be governed by Arizona's self-insurance statute A.R.S. § 41-621. The University of Arizona, as an agency of the State of Arizona, has no authority to use State funds to purchase insurance and any charges for insurance cannot be accepted.

I. **Governing Law.** This Agreement is made under and will be interpreted according to Arizona law.

Arizona Board of Regents	**XXX School District**
_____ Name	_____ Name
_____ Title	_____ Title
_____ Date	_____ Date

APPENDIX B
Cybersecurity Clinic Client Memorandum of Understanding

CYBERSECURITY CLINIC CLIENT
MEMORANDUM OF UNDERSTANDING

This Cybersecurity Clinic Client Memorandum of Understanding (this "Agreement") is effective as of the latest date of signature below (the "Effective Date") between the Arizona Board of Regents, acting for and on behalf of the University of Arizona (the "University") and XXX ("Client").

RECITALS

E. The University's College of Applied Science and Technology sponsors the Cybersecurity Clinic (the "Clinic"), wherein enrolled students obtain real world experience in the field under instructor supervision by providing local businesses with cybersecurity services.

F. Client would like to engage students in the Clinic to provide such cybersecurity services.

AGREEMENT

J. **Scope of Services**. The Clinic will assign a student team to assess Client cybersecurity risk and work collaboratively under instructor supervision to implement cybersecurity policies and technical controls to enhance Client's cybersecurity defenses (the "Services"). The Services will begin on [Date] and will continue for a period of [time] (the "Service Period").

K. **Payment**. There will be no payment required for the Services.

L. **Client Cooperation**.
   a. Client is expected to provide access to knowledgeable personnel for interviews, meetings, and work product reviews in a timely manner throughout the Service Period.
   b. Client agrees to share relevant requested information about organizational data, technology, activities, practices, processes, context, environment, etc., unless restricted by law. Client understands that pertinent information and data related to cybersecurity systems, protocols, personnel, past experiences, etc. are critical to the Clinic delivering an accurate and meaningful cybersecurity enhancement.

M. **Confidentiality**.
   a. Clinic staff and students will adhere to industry-standard cybersecurity protocols to keep Client data and communication secure.
   b. The Clinic will restrict Client information access to only current students on the Client's assigned team and the Clinic instructor.

N. **No Warranty; Disclaimer.**
   a. The Clinic will make reasonable efforts but cannot guarantee protection against security incidents such as unauthorized access to Client systems, disclosure of Client data, etc.
   b. The Clinic provides its services to Client on an "as is" and "as available" basis, with the express understanding that Clinic has no obligation to monitor or control Client's computing infrastructure, devices, practices, or data following the conclusion of the Service Period. As such, Client's use of Services is at its own discretion and risk.
   c. The Clinic makes no claims or promises about the quality, accuracy, or reliability of the Services, their safety or security, nor the program's content. Accordingly, the Clinic is not liable to Client for any loss or damage that might arise, for example, from the service or from any future security vulnerabilities. The Clinic expressly disclaims all warranties, whether express or implied, including implied warranties of merchantability, fitness for a particular purpose, and noninfringement.

O. **Limitation of Liability**

a. In no event will the Clinic be liable to Client or any third party for any indirect, incidental, special, consequential, or punitive damages arising out of or relating to the services or any materials or information that the Clinic provides, whether based on warranty, contract, tort (including negligence), statute, or any other legal theory, whether or not the Clinic has been informed of the possibility of such damages, except in proportion to and to the extent such liability, loss, expense, attorneys' fees, or claims for injury or damages are caused by or result from the negligent or intentional acts or omissions of the University, its officers, agents, or employees.
b. Client will not be liable to the Clinic for any indirect, incidental, special, consequential, or punitive damages arising out of or relating to the Client's engagement with the Clinic, except in proportion to and to the extent such liability, loss, expense, attorneys' fees, or claims for injury or damages are caused by or result from the negligent or intentional acts or omissions of the Client.

P. **Governing Law.** This Agreement is made under and will be interpreted according to Arizona law.

APPENDIX C
Student Non-Disclosure Agreement

University of Arizona Cybersecurity Clinic
Participant Non-Disclosure Agreement

By signing below, I, _____ agree to abide by the following during my participation in the Cybersecurity Clinic (the "Clinic").

Proprietary Information
I understand that by participating in the Clinic, I will have access to Proprietary Information (as defined below) belonging to local entities that engage the Clinic to provide cybersecurity assessments (each, a "Client" and collectively, the "Clients").

I agree to protect the confidentiality of all Proprietary Information disclosed to, shared with, or accessed by me during my work in the Clinic. Proprietary Information includes all data, materials, products, technology, computer programs, specifications, manuals, business plans, software, marketing plans, financial information, and other information disclosed or submitted, orally, in writing, or by any other media, to me by the Clinic or a Client.

I further agree to:

- Hold and maintain the Proprietary Information in the strictest confidence for the sole and exclusive benefit of the Clinic and the Clients.
- Not disclose, permit access to, or reveal the Proprietary Information to any third party without the prior written consent of the Clinic or the Client.
- Use the Proprietary Information only for the purpose of my work in the Clinic and not for any personal gain or detrimental purpose.
- Notify the Clinic immediately upon discovery of any unauthorized use or disclosure of Proprietary Information, whether by me or another Clinic participant.

Return of Proprietary Information
Upon the conclusion of my work with each particular Client, or upon request by the Clinic, I agree to return all copies of Client Proprietary Information to the Clinic or destroy such material, at the Clinic's discretion, and certify in writing that such return or destruction has been completed.

Remedies
I understand that any violation or threatened violation of this Agreement may cause irreparable injury to the Clinic and to the Client, and that they will be entitled to seek injunctive relief in addition to all legal remedies.

Participant Name _____

Signature _____

Date _____

APPENDIX D
Student Code of Conduct

University of Arizona
Cybersecurity Clinic Participant Code of Conduct

This Code of Conduct governs participation in the University of Arizona Cybersecurity Clinic. Participants who violate this Code of Conduct may be excluded from some or all Cybersecurity Clinic opportunities and events.

Clinic participants are expected to comply with the policies that govern all activities and behavior at the University of Arizona, in particular the Nondiscrimination and Anti-Harassment Policy, the Student Conduct policy, and the Acceptable Use of Computers and Networks Policy.
In addition, we expect all Clinic participants to abide by the following parameters:

- Be respectful to others. Do not engage in homophobic/homomesic, racist, transphobic/transmisic, ageist, ableist, sexist, or otherwise exclusionary behavior. Honor individuals' preferences for how they prefer to be addressed.
- Use welcoming and inclusive language. Exclusionary comments or jokes, threats or violent language are not acceptable while working in the Clinic. Do not address others in an angry, intimidating, or demeaning manner. Be considerate of the ways the words you choose may impact others. Be patient and respectful of the fact that English may be a second (or third or fourth!) language for Clinic participants.
- Do not harass people. Harassment includes unwanted physical contact, sexual attention, or repeated social contact. Know that consent is explicit, conscious and continuous—not implied. If you are unsure whether your behavior towards another person is welcome, ask them. If someone tells you to stop, do so.
- Respect the privacy and safety of others. Do not take photographs of others without their permission. Note that posting (or threatening to post) personally identifying information of others without their consent ("doxing") is a form of harassment.
- Be considerate of others' participation. Everyone should have an opportunity to be heard. While working in teams, please keep comments succinct so as to allow maximum engagement by all members. Be conscious and respectful of the fact that your team members may have different methods of communicating, and work to enable the most collaborative environment among your team.
- Don't be a bystander. If you see something inappropriate happening, speak up. If you don't feel comfortable intervening but feel someone should, please feel free to ask a member of the Clinic staff to intervene.
- As an overriding general rule, please be intentional in your actions and humble in your mistakes.

Operational Security
Working with the Cybersecurity Clinic will require engagement with its client organizations. These organizations and their staff, partners, and the communities they serve are often at risk of online or physical attacks. Therefore, adherence to Clinic operational security procedures is not just a requirement for academic success, but for safeguarding the lives and livelihoods of Clinic partners, students, staff, and their friends and families.
In order to facilitate a secure, safe working environment, all Clinic participants are expected to:

- Adhere strictly to any operational security requirements set for client communications by your team, by Clinic staff, or by the client.
- Do not seek to undermine existing security controls. Should you feel a security measure is ineffective, bring your concerns to Clinic staff before taking measures to alter any security systems or policies.
- Respect clients' perspectives. Even if we do not agree with a client's security concerns, we learn more about their security context by listening than telling. We do not know what we do not know.
- Keep track of any Clinic-owned devices assigned to you or your team. Ensure they are always under the control of you or your team, or are securely stored when not in use, and do not engage in any unlawful or unethical online or offline behavior with them. Do not change any

device settings in ways that would reduce device security. These devices are the gateway to our clients' and the Clinic's electronic infrastructure. You are the gatekeeper.
- Report any security incidents or concerns immediately to Clinic staff. This includes, but is not limited to, the loss, theft, or compromise of Clinic-owned devices or data stored on them.

Confidentiality
As a condition of allowing students to participate in the Clinic, including access to the Clinic's computers or other systems, all students agree to strictly protect any Confidential Information they receive as a result of their work with the Clinic. While the decision about whether information is "Confidential Information" depends on the specific information itself, some examples of Confidential Information include:
- The names of client organizations, their staff or clients, or other persons related to a Clinic project, or information likely to indicate identity.
- Any information related to organizational assessments or policy findings and recommendations.
- Any private communication or information regarding a specific client, a case, research data or analysis, including any underlying facts and circumstances not already revealed to the public.
- Any report or other written material, including that which the undersigned or their team has drafted, unless such document has been approved for release and properly redacted by a member of the Clinic supervising faculty or professional staff; and
- Identities or other personal information about clients required by applicable research protocols to remain confidential to minimize the risk to research subjects of participation in research.

The undersigned student agrees that they will not violate the confidentiality of the Clinic's interests or those of the Clinic's clients by revealing Confidential Information to those outside the Clinic. By signing this Agreement, the student agrees not to disclose Confidential Information orally or in writing, including through electronic media or any online forum, and not to write about any aspect of a Clinic case or project in any print or online publication without the express, prior permission of the Clinic's supervising faculty or professional staff. The obligation of each student to maintain the confidentiality of information is on-going and continues after the student's participation in the Clinic has ended. Clinic faculty and professional staff are available to answer any questions or concerns about this Agreement, or about disclosure of any specific information. Students who are uncertain about whether certain information is Confidential Information should ask mentors, Clinic faculty or professional staff before any disclosure.

Professionalism
Working with client organizations is a position of significant privilege and trust. Your work does not just represent you, but your team, the Cybersecurity Clinic, the College of Applied Science and Technology, and the University of Arizona at-large. Students are expected to be on time to all client meetings and to be attentive and respectful during all external-facing engagements.
Work product, communications, and other client-facing materials you may produce over your time with the Clinic must adhere to a very high standard of quality. The work that is done in this Clinic varies from team to team, but always keep in mind these three characteristics when preparing work for clients:
- **Rigor:** Be thorough in your research. Do not make recommendations for clients based on what you assume they need—all recommendations should have a rigorous explanation behind them.
- **Attention to Detail:** Spelling, grammar, design, organization—do not underestimate the importance of details. We want clients to rely on the materials we create when they are considering meaningful decisions about their security. Bad writing does not instill confidence.
- **Contextualize:** Think about who your audience is for any document or deliverable—whether it is an email, an organizational policy, or a report. Who is reading it? Who might read it? How technical are they? Do they read English? How well? Tailoring your work to your audience is critical to making the work meaningfully received and understood.

The undersigned agrees to abide by the terms of this Code of Conduct for the duration of their involvement with the Cybersecurity Clinic. Failure to do so may result in disciplinary action outlined within the code, or as required by University of Arizona policy.

Your Name (Printed): _____

Your Signature: _____

Date: _____

APPENDIX E
Client Intake Form

1. Company Information
Company Name:
Business Address:
Industry Sector:
Primary Contact:
Name:
Title:
Email:
Phone:
Secondary Contact (if applicable):
Name:
Title:
Email:
Phone:
Number of Employees:
Location(s) of Offices / Operations:
Website:
Social Media:
LinkedIn:
Instagram:
X:
Facebook:
TikTok:
Other:
Key Products or Services Offered by your organization:

1a. What services are you looking to obtain from the Arizona Cybersecurity Clinic?:
☐ Cybersecurity Awareness Training
☐ Cybersecurity Risk Assessment
☐ Organizational Research using Open Search Intelligence (OSINT)
☐ Website Vulnerability Assessment

1b. Have there been any recent security incidents or data breaches? If so, could you briefly describe them?

1c. What ongoing cybersecurity concerns or threats have been observed?

1d. What are the primary goals of the cybersecurity program (e.g., risk reduction, compliance, etc.)?

2. Security Policies and Procedures
2a. What are the current cybersecurity policies you have in place (if any)?

☐ Incident Response	☐ Acceptable Use
☐ Remote Access	☐ Network Security
☐ Data Management	☐ Disaster Recovery
☐ Employee Awareness	☐ Data Backup
☐ Vendor Management	☐ Data Retention
☐ Email	☐ Risk Management
☐ Change Management	☐ Access Control
☐ Password	☐ Vendor / Contractor
☐ BYOD	☐ Other

Please attach / provide your current policies and any specific procedures.

2b. Does your organization offer any employee training?
Annotate how often all employees are required to conduct training:
0 = No Current Requirement; 1 = Annually; 2 = Semi-annually; 4 Quarterly

Information Security	Mobile Security
Social Engineering	Phishing
Physical Security	Wireless
Security Awareness	Safe Internet
Email Security	Other

Please attach current links or documents on the required training.

3. Data and Information Management

3a. What types of data do you manage?

☐ Biometric	☐ Privacy
☐ Health	☐ Business
☐ Financial	☐ Intellectual Property
☐ Credit Card	☐ Classified / Sensitive
☐ Bank Account	☐ Trade Secrets
☐ Email Addresses	☐ Consumer (Name / Address / Phone, etc.)
☐ Membership	☐ Other

3b. Where is data stored?
☐ On-Premises (Physical)
☐ On-Premises (Digital)
☐ Cloud
☐ 3rd Party Data Center
☐ Other

3c. If your organization utilizes data backup solutions, where is the data stored?
☐ On-premises
☐ Cloud
☐ 3rd Party Data Center
☐ Other
☐ Unknown
☐ No data backup solution

3d. Are tests completed annually of data backup systems?
☐ Yes
☐ No
☐ Unknown

3e. If you have a data retention policy, is it being followed?
☐ Yes
☐ No
☐ Unknown

3f. Is your organization utilizing access control?
☐ Yes
☐ No
☐ Unknown

3g. If utilizing an access control, what type is it?

☐ Role Based	☐ Attribute-Based
☐ Mandatory	☐ Discretionary
☐ Rule Based	☐ Other

3h. Is access to sensitive information restricted based on a need-to-know basis?
☐ Yes
☐ No
☐ Unknown

3i. Are access controls reviewed and updated regularly?
☐ Yes
☐ No
☐ Unknown

3j. Do you maintain logs of access to sensitive information?
☐ Yes
☐ No
☐ Unknown

3k. Are user accounts regularly reviewed for necessary permissions?
☐ Yes
☐ No
☐ Unknown

3l. Are inactive accounts disabled promptly?
☐ Yes
☐ No
☐ Unknown

3m. Do you monitor and log account activity, especially for privileged accounts?
☐ Yes
☐ No
☐ Unknown

4. Network Security and Access Control
4a. Does your organization utilize any of the following network hardware? (Please denote type)
Network Equipment:

Load Balancer	NAC	UTM
IDS / IPS	VPN	SIEM
Web Filter	Switch	Router
Wi-Fi AP	Modem	Bridge
Repeater	Hub	Gateway
Other		

Server:

Mail	DHCP	Web
File	Database	Print
Application	Proxy	Reverse Proxy
FTP	DNS	Fax
Virtual	Cloud	Other

Firewall:

Stateful	Stateless	NGFW
WAF	Cloud	Packet Filtering

IPS:
☐ Network
☐ Host
☐ WIPS
☐ Other

IDS:
☐ Network
☐ Host
☐ WIDS
☐ Other

SIEM:
☐ Snort
☐ Splunk
☐ Qradar
☐ LogRhythm
☐ Other

EDR **XDR** **Email Security**

Please provide a detailed list of security assets, including make, model, version, and serial number.

4b. Do you use network segmentation (e.g., separate networks for different data types or roles)?
☐ Yes
☐ No
☐ Unknown

4c. Is Multi-Factor Authentication (MFA) utilized?
☐ Yes
☐ No
☐ Unknown

4d. How many clients (computers, tablets, cell phones) are currently being utilized in your organization?
☐ 1 – 20
☐ 21 – 50
☐ 51 – 100
☐ 101 – 250
☐ 251 - 500
☐ 501+

4e. Do employees use personally owned devices to conduct business functions?
☐ Yes
☐ No
☐ Unknown

4f. Does your organization use a password manager?
☐ Yes
☐ No
☐ Unknown

4fi. If so, which one is being used?

5. Wireless
5a. Does your organization utilize Wi-Fi?
☐ Yes
☐ No
☐ Unknown

5b. Are guests allowed to access your network?
☐ Yes
☐ No
☐ Unknown

5bi. If yes, do you have a separate network for them to connect to?
☐ Yes
☐ No
☐ Unknown

5c. If Wi-fi is being utilized what encryption is being used?
☐ WEP
☐ WPA Personal
☐ WPA2 Personal
☐ WPA3 Personal
☐ WPS
☐ WAP Enterprise
☐ WPA2 Enterprise
☐ WPA3 Enterprise
☐ Unknown

6. Endpoint and Application Security
6a. Is your organization utilizing a 3rd party Antivirus program? (Not Windows Defender)
☐ Yes
☐ No
☐ Unknown

6b. If using a 3rd party AV, is it the free version?
☐ Yes
☐ No
☐ Unknown

6c. If using a 3rd party AV, please denote which one.
☐ Norton
☐ McAfee
☐ CrowdStrike
☐ AVAST
☐ Bitdefender
☐ Malware Bytes
☐ Sophos
☐ Other

6d. Does your organization utilize application listing?
☐ Yes
☐ No
☐ Unknown

6di. If yes, what type?
☐ Block / Blacklisting
☐ Allow / Whitelisting
☐ Unknown

6e. What is the frequency of your organization's patch management?
☐ Weekly
☐ Quarterly
☐ Bi-Weekly
☐ Annually
☐ Monthly
☐ Other
☐ Unknown

7. Compliance and Regulatory Requirements
7a. Are there any industry-specific compliance requirements?
☐ GDPR
☐ SOX
☐ FERPA
☐ PCI-DSS
☐ SOC 2
☐ GLBA
☐ FISMA
☐ HIPAA
☐ CCPA
☐ CMMC
☐ Other
☐ Unknown

7b. Does your organization perform annual security audits?
☐ Yes
☐ No
☐ Unknown

Please provide the compliance requirements for third-party vendors if applicable.

7c. Is sensitive data identified and classified?
☐ Yes
☐ No
☐ Unknown

7d. Are controls in place to prevent unauthorized access to sensitive data?
☐ Yes
☐ No
☐ Unknown

7e. Is data encrypted during transit and at rest?
☐ Yes
☐ No
☐ Unknown

8. Inventory and Control Software Assets
8a. Is there an up-to-date inventory of all installed software?
☐ Yes
☐ No
☐ Unknown

8b. Are unauthorized software installations detected and resolved promptly?
☐ Yes
☐ No
☐ Unknown

8c. Do you regularly review and validate the software inventory for compliance?
☐ Yes
☐ No
☐ Unknown

9. Continuous Vulnerability Management
9a. Do you conduct regular vulnerability scanning on all systems?
☐ Yes
☐ No
☐ Unknown

9b. Is there a process for timely remediation of identified vulnerabilities?
☐ Yes
☐ No
☐ Unknown

9c. Are vulnerability scan reports reviewed and acted upon regularly?
☐ Yes
☐ No
☐ Unknown

10. Controlled Use of Administrative Privileges
10a. Are administrative privileges granted only based on roles and responsibilities?
☐ Yes
☐ No
☐ Unknown

10b. Do you track and audit the use of administrative privileges?
☐ Yes
☐ No
☐ Unknown

10c. Is there a process to revoke administrative privileges when they are no longer required?
☐ Yes
☐ No
☐ Unknown

11. Secure Configuration for Hardware and Software
11a. Are secure configurations applied to all hardware and software upon installation?
☐ Yes
☐ No
☐ Unknown

11b. Do you regularly update and validate secure configurations?
☐ Yes
☐ No
☐ Unknown

11c. Are deviations from secure configurations detected and corrected promptly?
☐ Yes
☐ No
☐ Unknown

12. Email and Web Browser Protections

12a. Do you have mechanisms to filter out malicious email and web content?
☐ Yes
☐ No
☐ Unknown

12b. Are email and web browser security settings configured and regularly updated?
☐ Yes
☐ No
☐ Unknown

12c. Do you regularly train employees on email and web security best practices?
☐ Yes
☐ No
☐ Unknown

13. Limitation and Control of Network Ports, Protocols, and Services

13a. Are unnecessary network ports, protocols, and services disabled on all systems?
☐ Yes
☐ No
☐ Unknown

13b. Is there a process to regularly review and validate network port, protocol, and service configurations?
☐ Yes
☐ No
☐ Unknown

13c. Do you monitor and log network port, protocol, and service activities?
☐ Yes
☐ No
☐ Unknown

14. Secure Configuration for Network Devices

14a. Are secure configurations applied to network devices such as firewalls, routers, and switches?
☐ Yes
☐ No
☐ Unknown

14b. Do you regularly review and update network device configurations?
☐ Yes
☐ No
☐ Unknown

14c. Does your organization regularly utilize a vulnerability scanner to identify configuration faults?
☐ Yes
☐ No
☐ Unknown

14d. If so, what type? Please provide the latest report if available.
☐ Nessus
☐ OpenVas
☐ Other
☐ Unknown

14d. Are changes to network device configurations logged and audited?
☐ Yes
☐ No
☐ Unknown

15. Penetration Tests and Red Team Exercises
15a. Do you conduct regular penetration tests to evaluate security?
☐ Yes
☐ No
☐ Unknown

15b. Are results from penetration tests used to improve security measures?
☐ Yes
☐ No
☐ Unknown

15c. Do you employ red team exercises to simulate real-world attacks?
☐ Yes
☐ No
☐ Unknown

Acronyms and Glossary

AP – Access Point – A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise wired network.

Attribute-Based Access Control (ABAC) – An access control approach in which access is mediated based on attributes associated with subjects (requesters) and the objects to be accessed. Each object and subject have a set of associated attributes, such as location, time of creation, access rights, etc. Access to an object is authorized or denied depending upon whether the required (e.g., policy-defined) correlation can be made between the attributes of that object and of the requesting subject.

Blacklisting – The process used to identify: (i) software programs that are not authorized to execute on an information system; or (ii) prohibited universal resource locators (URL)/websites.

BYOD – Bring Your Own Device – A policy that allows employees to use their own devices for work. The devices can include smartphones, tablets, laptops, and USB drives

CCPA – California Consumer Privacy Act – Law that secures privacy rights for California consumers, including: the right to know about the personal information a business collects about them and how it is used and shared; the right to delete personal information collected from them (with some exceptions); the right to opt-out of the sale or sharing of their personal information; and the right to non-discrimination for exercising their CCPA rights.

CMMC – Cybersecurity Maturity Model Certification – An assessment framework developed by the U.S. Department of Defense (DoD) with the primary objective to enhance cybersecurity controls in place for organizations supplying the DoD, known as the Defense Industrial Base (DIB). The CMMC model aims to manage risk and verify that DoD contractors can safeguard information classed as Controlled Unclassified Information (CUI) and comply with NIST SP 800-171 DoD assessment requirements and other cybersecurity requirements.

Controlled Unclassified Information (CUI) – Information that the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

Defense Industrial Base (DIB) – The Defense Industrial Base Sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements.

DHCP – Dynamic Host Configuration Protocol – A network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client–server architecture.

Discretionary Access Control (DAC) – An access control policy that is enforced over all subjects and objects in a system where the policy specifies that a subject that has been granted access to information can do one or more of the following: pass the information to other subjects or objects; grant its privileges to other subjects; change the security attributes of subjects, objects, systems, or system components; choose the security attributes to be associated with newly-created or revised objects; or change the rules governing access control. Mandatory access controls restrict this capability.

DNS – Domain Name System – A hierarchical and distributed name service that provides a naming system for computers, services, and other resources on the Internet or other Internet Protocol (IP) networks.

EDR – Endpoint Detection & Response – A cybersecurity technology that continually monitors an "endpoint" (e.g. a client device such as a mobile phone, laptop, Internet of things device) to mitigate malicious cyber threats.

Federal Educational Rights and Privacy Act – A United States federal law that governs the access to educational information and records by public entities such as potential employers, publicly funded educational institutions, and foreign governments.

FISMA – Federal Information Security Management Act – A law that protects the government's information, assets, and operations from threats. The law was originally passed in 2002 as the Federal Information Security Management Act but was updated in 2014 in response to a growing number of cyber-attacks on the federal government.

FTP – File Transfer Protocol – A standard for transferring files over the internet. FTP programs and utilities are used to upload and download web pages, graphics, and other files between local media and a remote server that allows FTP access.

GDPR – General Data Protection Regulation – A European Union law that protects the privacy and security of personal data. It applies to all EU member states and the European Economic Area (EEA).

GLBA – Gramm-Leach-Bliley Act – A law that requires financial institutions to protect consumer information. The law was enacted in 1999 and is also known as the Financial Services Modernization Act.

HIPAA – Health Insurance Portability & Accountability Act – Establishes federal standards protecting sensitive health information from disclosure without patient's consent.

IDS – Intrusion Detection System – A software application or device that monitors a network or system for malicious activity or policy violations. IDSs are a key component of network security defenses and can help identify security incidents, bugs, and device configuration issues.

IPS – Intrusion Prevention System – A network security tool that monitors network activity for malicious activity and takes action to prevent it

MFA – Multi-Factor Authentication – An authentication system that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

NAC – Network Access Control – A computer security method that limits access to a network by unauthorized devices and users. NAC uses rules, protocols, and processes to control access to network resources, such as PCs, IoT devices, and network routers. It also applies to data and resources transmitted through the network, as well as virtual and software-defined resources.

NGFW – Next Generation FireWall – A cybersecurity tool that protects networks from cyber threats by combining traditional firewall technology with other network filtering functions. NGFWs can block modern threats like advanced malware and application-layer attacks, and they can also receive and act on threat intelligence feeds from external sources.

PCI-DSS – Payment Card Industry Data Security Standard – A set of guidelines that protect cardholder data and account information. The Payment Card Industry Security Standards Council (PCI SSC) creates and enforces the standard. PCI-DSS protects credit card information, prevents unauthorized access to account data, helps businesses detect and respond to security failures, helps businesses maintain security awareness, and helps businesses monitor and adapt to changes in cybersecurity threats.

Proxy – An application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. Note: This effectively closes the straight path between the internal and external networks making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, a hypertext transfer protocol (HTTP) proxy used for Web access, and a simple mail transfer protocol (SMTP) proxy used for e-mail.

Role Based Access Control (RBAC) – Access control based on user roles (i.e., a collection of access authorizations that a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

Rule Based Access Control - Access control model that regulates user access to computer or network resources based on predefined rules aligned with the user's job functions and organizational structure. Instead of granting permissions directly to individual users, RBAC assigns user permissions based on their assigned roles. This streamlines access management and simplifies security policy enforcement.

SOC 2 – Service Organization Control – A report that can be provided to third parties to demonstrate a strong control environment; an audit performed by a third-party auditor (CPA) to provide said report; or the controls and "framework" of controls that allow an organization to attain a SOC 2 report. In other words, SOC 2 is a "report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy.

SOX – Sarbanes-OXley Act – A United States federal law designed to further protect shareholders and the public from general accounting fraud in public and private companies by improving the accuracy of corporate disclosures.

SIEM – Security Information and Event Management – Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface

Stateful Firewall – A firewall that keeps track and monitors the state of active network connections while analyzing incoming traffic and looking for potential traffic and data risks. This firewall is situated at Layers 3 and 4 of the Open Systems Interconnection (OSI) model.

Stateless Firewall – A type of firewall that filters network traffic based on individual packets without storing information about the state or context of connections. When comparing stateless vs. stateful firewalls, stateless firewalls make filtering decisions based only on the information present in each packet as opposed to stateful firewalls, which maintain a state table.

UTM – Unified Threat Management – Provides multiple security features and services in a single device or service on the network, protecting users from security threats in a simplified way. UTMs includes functions such as anti-virus, anti-spam, content filtering, and web filtering. Also known as a Next Generation Firewall (NGFW).

VPN – Virtual Private Network – A virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and IP information transmitted between networks or between different nodes on the same network.

WAF – Web Application Firewall – A security tool for monitoring, filtering and blocking incoming and outgoing data packets from a web application or website. WAFs can be host-based, network-based or cloud-based and are typically deployed through reverse proxies and placed in front of an application or website (or multiple apps and sites).

WEP – Wired Equivalent Privacy – Security protocol specified in the IEEE Wireless Fidelity (Wi-Fi) standard 802.11b.

Whitelisting – An implementation of a default deny all or allow by exception policy across an enterprise environment, and a clear, concise, timely process for adding exceptions when required for mission accomplishments.

WIDS – Wireless Intrusion Detection System – a technology designed to protect wireless networks from unauthorized access. It does this by monitoring traffic on the network to identify any suspicious activity that may indicate a security breach.

WIPS – Wireless Intrusion Prevention System – A technology designed to protect wireless networks from unauthorized access using a combination of techniques to detect and prevent intrusions in real time. It not only monitors but also takes action to prevent rogue access points, man in the middle attacks, denial-of-service attacks, and other threats to the wireless network.

WPA – Wi-Fi Protected Access – A security protocol that protects wireless networks by using encryption and authentication to limit access to authorized users

WPS – Wi-Fi Protected Setup – A wireless security standard that allows users to connect devices to a network without entering a password. WPS is designed to simplify the process of setting up a secure wireless network, especially for users who are unfamiliar with wireless security.

XDR – eXtended Detection & Response – A cybersecurity solution that combines security tools into a single platform to detect and respond to threats. XDR can collect data from a variety of sources, including endpoints, networks, cloud workloads, and email, and use AI and automation to analyze it. This allows security teams to more quickly and accurately identify threats and resp

What is Cybersecurity (or Cyber Security)? Answer [Still] Loading…

Maguire Parsley
map3454@uncw.edu

Luke Warpula
lcw7948@uncw.edu

Ulku Clark
clarku@uncw.edu

Geoff Stoker
stokerg@uncw.edu

Congdon School
University of North Carolina Wilmington
Wilmington, NC 28403 USA

Abstract

A quote attributed to Bertrand Russell states that, "In all affairs, it's a healthy thing now and then to hang a question mark on the things you have long taken for granted." Perhaps it is even healthier to regularly inquire about things that are yet unsettled. This paper reports on our search for the first use of the term cyber security, our analysis of the current preference of the one-word (cybersecurity) vs. two-word (cyber security) form of the term, and our investigation into literature from academia, government, and the business world to determine the current state of definitions. The best evidence we found indicates that the 1990 book Kaduna Memories by Jack McKinney (a pseudonym for authors James Luceno and Brian Daley) contains the first use of the term cyber security. Though use of the two-word version, cyber security, came first, we found that the one-word version has gained acceptance and is now ascendant. Unsurprisingly, although the 60 definitions we examined share a common theme, there are sufficient differences among them that consensus seems to be somewhere in the future. Synthesizing what we found, cybersecurity today might reasonably be considered *the practice of protecting digital data, computer systems, information technology, and networks against attacks, threats, and unauthorized access*. Conspicuously absent from this synthesis is the word "risk," which seems likely to gain acceptance in future cybersecurity definitions as the domain continues to mature.

Keywords: Cybersecurity, Cyber Security, Literature Review, Definition

Recommended Citation: Parsley, M., Warpula, L., Clark, U.Y., Stoker, G., (2026). What is Cybersecurity (or Cyber Security)? Answer [Still] Loading. *Cybersecurity Pedagogy and Practice Journal;* v5(n2) pp 34-58. DOI# https://doi.org/10.62273/HGTQ7475

What is Cybersecurity (or Cyber Security)? Answer [Still] Loading…

Maguire Parsley, Luke Warpula, Ulku Clark, and Geoff Stoker

1. INTRODUCTION

At the 4th annual Cybersecurity Symposium hosted by the North Carolina Partnership for Cybersecurity Excellence, 16-17 April 2025, an 11-person panel presented, "Hack the Gap: Shaping Tomorrow's Cybersecurity Workforce" (North Carolina Partnership for Cybersecurity Excellence, 2025). One panelist, who worked in the private sector and had hiring experience, expressed frustration with the lack of a common understanding of the term cybersecurity. He was unsure what a B.S. in Cybersecurity implied for recipients' skills and abilities. In reaction, another panelist concisely and confidently stated that cybersecurity was the "application of risk management to digital assets" (K. Robinson, personal communication, April 17, 2025).

This discussion prompted us to wonder to what extent a definition of cybersecurity had converged and to be curious about the origin of the term cybersecurity. A Google search of "who first coined the term cybersecurity" resulted in the Google-AI response: "The term 'cybersecurity' was first coined by William Gibson in 1983, in his novel Neuromancer" (Google, 2025). Temporarily gratified by this definitive result, we were subsequently a bit surprised when a search of an online copy of Gibson's novel revealed that while the word "cyberspace" shows up 24 times, neither "cyber security" nor "cybersecurity" is anywhere to be found (Gibson, 1984). Encountering this unexpected result motivated further exploration and, ultimately, the writing of this paper.

In this investigation, we set out to answer the following research questions (RQ):

RQ1: When was the term cyber security first used?
RQ2: Which form of the term is currently most accepted (cyber security or cybersecurity)?
RQ3: What is the current state of definitional consensus for the term cybersecurity?

Section 2 surveys prior attempts to define cybersecurity and identifies a gap: no existing work compares definitions across the dictionary, governmental, academic, industry, and GenAI domains simultaneously. Section 3 details our methods for closing that gap; Section 4 presents our comparative analysis of 60 definitions collected across those domains; Section 5 concludes.

2. BACKGROUND & RELATED WORK

Wrestling to understand and define the scope of an emerging field is neither new nor unique to cybersecurity. For example, the field of computer science has been the subject of debate about its essence since the 1930s. All it seemingly takes to glimpse this continuing struggle is to ask a group of computer scientists what they think of the quote, popularly attributed to Edsger Dijkstra, that "computer science is no more about computers than astronomy is about telescopes" (Computer Science Is Not about Computers, Any More than Astronomy Is about Telescopes – Quote Investigator, n.d.). Practitioners have long debated the heart of computer science – is it primarily about algorithms, machines, information processes, or something else (Denning, 2008)? Perhaps the most famously useful, albeit general and somewhat circular, definition is, "Computer science is the study of the phenomena surrounding computers" (Newell et al., 1967).

Seeking a Cybersecurity Definition

We are not the first to seek clarification on the term "cybersecurity," and we do not expect to be the last. Craigen et al. (2014) conducted an in-depth literature review and led discussions with practitioners, academics, and graduate students to arrive at their definition: "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" (p. 1).

The European Union Agency for Network and Information Security (ENISA) [Note: ENISA is now called the European Union Agency for Cybersecurity], responding to a recommendation to establish a "clear and common understanding of the scope of Cyber Security" (European Union Agency for Cybersecurity, 2015, p. 8), published a report in 2015. In it, they identified five different domains often included under cyber-security: communications security, operations

security, information security, military security, and physical security. They ended up concluding that a definition is unnecessary for application to simple things like identity authentication and that "the problem is that Cybersecurity is an enveloping term and it is not possible to make a definition to cover the extent of the things Cybersecurity covers" (European Union Agency for Cybersecurity, 2015, p. 28).

In a search for an encompassing definition of cybersecurity, Bay (2016) opined that, "a very precise definition of the term cybersecurity that can be summed up in a few sentences seems quite elusive" (p. 23). Though some use terms like computer security and cybersecurity interchangeably, he argued that while computer security and information security overlap with cybersecurity, they are not the same thing. He concluded that, "cybersecurity is a security matter which spans from the individual's security against cyber threats to all of society. As such, the concept of cybersecurity demands a multi-faceted theoretical approach" (Bay, 2016, p. 24).

Studies have shown that established knowledge frameworks interpret cybersecurity as involving a variety of non-technical topics (Furnell & Collins, 2021) (see Figure 1). As noted by Siudak (2022, p. 1), "there is no single universal understanding of cybersecurity." Additionally, recent research has aimed to explore non-expert definitions of cybersecurity (Neil et al., 2023).

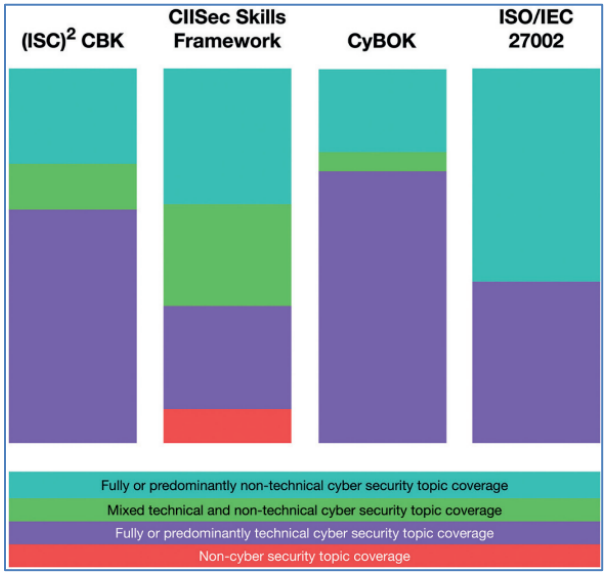


Figure 1: Part of Furnell & Collins' Figure 2 (2021) showing topic coverage for well-known knowledge frameworks (top portion represents non-technical topic coverage).

These prior efforts, spanning academic literature reviews (Craigen et al., 2014; Bay, 2016), governmental and standards bodies (European Union Agency for Cybersecurity, 2015), and knowledge-framework studies (Furnell & Collins, 2021; Siudak, 2022), illustrate that the search for a common definition has been narrow in scope, typically drawing on a small, single-category set of sources. None systematically compares definitions across the dictionary, government, academic, industry, and GenAI domains at once. That broader, cross-domain comparison, encompassing the 60 definitions analyzed in Section 4, is this paper's contribution.

3. METHODOLOGY

For this investigation, we conducted a literature review and analysis to identify the earliest use of either "cyber security" or "cybersecurity," determine which form is currently preferred, and collect and analyze current definitions from multiple sources to assess the level of definitional consensus.

Term Origin

While cybersecurity-related activities have presumably been ongoing since the early days of the electronic computer age, we focused on identifying the earliest use of the term itself. We began with a broad search using Google and our institution's library discovery platform, which surfaces results across hundreds of English-language archive databases. Initial results guided further targeted searches across more than 50 individual databases, which yielded potentially relevant material. This process led us beyond the well-known periodicals, aggregation databases, and technical publications we expected to be most relevant — such as the Association of Computing Machinery (ACM) Digital Library, Chicago Tribune, Christian Science Monitor, Institute of Electrical and Electronic Engineers (IEEE) Xplore, Los Angeles Times, New York Times, NIST publications, Wall Street Journal, and Washington Post archives — to smaller regional sources as well. Notably, the earliest periodical use of "cyber security" we found was not in any of these prominent outlets but in *The Dispatch-Argus* in Moline, Illinois (see Table A-1).

Term Preference

Is it cyber security or cybersecurity? [Note: cyber security and the hyphenated, cyber-security, were treated as the same form.] Of course, it is both, but as we searched for the first uses of the term, we looked for both forms to see which appeared earlier in each source we examined. We also used Google Trends and Google Books

Ngram Viewer to examine the prevalence of the two forms of the term over time.

Definitions
We collected definitions for cybersecurity across several different collections – online dictionaries, governmental organizations, standards organizations, published academic papers, generative AI tools, and tech companies.

Dictionaries
We conducted Google searches to determine available, popular, and respected online dictionaries, and then collected definitions from eight (8): Cambridge, Collins, Dictionary.com, Merriam-Webster, Oxford English Dictionary (OED), Urban Dictionary, Wiktionary, and WordWeb Online.

Governmental and Standards Organizations
We collected definitions from eight (8) documents from six (6) sources: the Congressional Research Service (CRS), the Cybersecurity & Infrastructure Security Agency (CISA), the European Union Agency for Cybersecurity (ENISA), the International Organization for Standardization (ISO), the Joint Task Force (JTF) on Cybersecurity Education [a collaboration of the Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE), Association of Information Systems (AIS), and the International Federation for Information Processing (IFIP)], and the National Institute of Standards and Technology (NIST).

Tech Companies
To gather cybersecurity definitions from the corporate world, we focused on large tech companies. We examined the largest tech companies by market capitalization (Companies Marketcap, n.d.). Given AI's demonstrated unreliability in making factual claims (see Section 1), we used ChatGPT only to locate candidate sources, never as the source of a definition itself; every definition was independently verified against its original primary-source text before inclusion. For each company, we prompted ChatGPT, "does company XXX have any official definition of cybersecurity. Provide a source." If no definition was found, we skipped the company. For the others, we visited the link provided by ChatGPT to verify the definition's existence and copied it directly from the company's website. Definitions were copied from 10 companies: Microsoft, Google, Amazon, Broadcom, SAP, AMD, Cisco, Salesforce, IBM, and ServiceNow.

Cybersecurity Companies
To gather definitions from the corporate cybersecurity world, we followed the same methodology as for tech companies. We looked at the largest cybersecurity companies by market capitalization (Companies Marketcap, n.d.) and prompted ChatGPT with the exact same prompt, "Does company XXX have any official definition of cybersecurity. Provide a source." If no definition was found, we skipped the company. For the others, we visited the link provided by ChatGPT to verify the definition's existence, then copied it directly. Definitions were collected from 10 companies: Palo Alto Networks, CrowdStrike, Fortinet, Cloudflare, Zscaler, Okta, F5, Akamai, SailPoint, and SentinelOne.

Academic Papers
Our entry point to this investigation was Bay's paper, "What is Cybersecurity?" (2016), from an initial Google Scholar search. From this paper, we conducted a snowball search: looking backward in time through cited works and forward in time using Google Scholar's "cited by" feature, then repeating this process for each newly identified work that clearly presented a definition of cybersecurity. We continued this process until it stopped surfacing sources meeting that inclusion criterion, at which point seven (7) qualifying sources had been identified; this number was therefore a result of the method rather than a predetermined target. Each definition was extracted verbatim. Since Bay's paper concluded with, "a very precise definition of the term cybersecurity that can be summed up in a few sentences seems quite elusive" (2016, p. 23), we do not include a definition from his work.

Universities
To gather university definitions of cybersecurity, we conducted a web-based review targeting top cybersecurity institutions. We used EduRank's "Best Universities for Cyber Security in the World" (2025) to source definitions. For each, we recorded the university name, URL, and quoted text. Definitions were collected from 10 of the top universities: the University of California, Berkeley; Stanford; MIT; Carnegie Mellon; the University of Cambridge; Georgia Tech; Harvard; the University of Illinois Urbana-Champaign; UT Austin; and NYU.

Generative AI
To gather definitions from Generative AI, we asked seven of the top Large Language Models (LLMs), "What is the best general, concise definition of cybersecurity?" After documenting the response, we then asked the LLM, "Did you make this definition up or was it collected from documents?" Most LLMs listed the sources used to generate the definition provided. Some

required further questioning to identify the sources used; we asked, "What sources did you use to construct your definition?" We consulted seven (7) LLMs: ChatGPT, Microsoft CoPilot, Google Gemini, Claude, DeepSeek, Meta AI, and Perplexity – only Claude was unable to provide a source used for its definition.

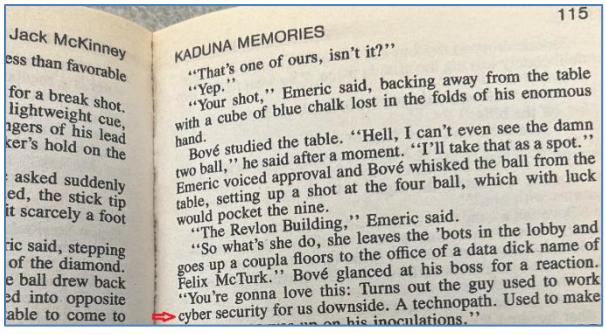
Term Frequencies

To find the frequently used words among the sections of definitions, we used WriteWords Word Frequency Counter (http://www.writewords.org/uk/word_count.asp). We gathered all definitions from each subsection and documented all words with two or more instances. Additionally, we removed redundant filler words such as "I," "and," and "the." For some sections, we combined words like system and systems into a single word, system(s), to improve analysis. For each source category, we visualized these results as a bar graph. We then repeated the same process on the full combined set of 60 definitions across all categories, producing an aggregate bar graph, and additionally isolated the 30 most frequent words from that combined set in a separate bar graph for closer analysis.

4. LITERATURE REVIEW, ANALYSIS, & FINDINGS

Term Origin

In Table A-1, we provide examples of the earliest use of the term cyber security that we could find across a variety of publicly available English-language sources. None of the sources provided an earlier use of "cybersecurity," so only "cyber security" references are provided. The best evidence we could find indicates that "cyber security" was first used by McKinney (pseudonym) in the science fiction book, Kaduna Memories (1990) (Figure 2) [RQ1].


Jack McKinney
ess than favorable
for a break shot.
lightweight cue,
ngers of his lead
ker's hold on the
asked suddenly
ed, the stick tip
it scarcely a foot
ric said, stepping
of the diamond.
e ball drew back
ed into opposite
able to come to

115

KADUNA MEMORIES

"That's one of ours, isn't it?"

"Yep."

"Your shot," Emeric said, backing away from the table with a cube of blue chalk lost in the folds of his enormous hand.

Bové studied the table. "Hell, I can't even see the damn two ball," he said after a moment. "I'll take that as a spot." Emeric voiced approval and Bové whisked the ball from the table, setting up a shot at the four ball, which with luck would pocket the nine.

"The Revlon Building," Emeric said.

"So what's she do, she leaves the 'bots in the lobby and goes up a coupla floors to the office of a data dick name of Felix McTurk." Bové glanced at his boss for a reaction. "You're gonna love this: Turns out the guy used to work cyber security for us downside. A technopath. Used to make

Figure 2: "cyber security" appears in Kaduna Memories (1990), p. 115.

Our search for the origin of the term was more difficult than anticipated. As indicated in the introduction, Google Search AI unequivocally attributed the first use of the term "cybersecurity" to William Gibson in his 1983 novel Neuromancer (Google, 2025), and this is not correct. Over the course of our search for the first use of the term, Google Search AI's answer evolved. The same search on June 5, 2025, provided this result:

> The term "cybersecurity" is often associated with William Gibson, a science fiction author, due to his use of the term "cyberspace" in his 1980s works like "Neuromancer". While Gibson's work popularized the concept of a virtual space and its associated risks, there's no conclusive evidence that he was the first to use the term "cybersecurity" in a technical context. (Google, 2025)

In response to the slightly different prompt, "Who first used the term cyber security or cybersecurity?" Microsoft's Copilot provided this response: "The term 'cybersecurity' was first recorded in 1989, according to linguistic and historical sources" (Copilot, 2025). Pulling the 1989 thread by following the Copilot-provided sources, we found websites that claimed the term dates back to 1989 (Gologanoff, 2023; Kinsella, 2022; Lal, 2023), but did not find any evidence of the term's actual use in that year. The Merriam-Webster dictionary provides a self-referential citation under the Word History section: "First known use 1989, in the meaning defined above" (Merriam Webster, 2019).

One interesting story discovered in our search for the first use of cyber security involved Jamie Gorelick, the former US Deputy Attorney General during the Clinton Administration. In a 2016 interview reflecting on her service, she stated, "By that point, we came up with a name for the threat, which was cyber security. We named it" (Jamie Gorelick Discusses the Birth of Cybersecurity, 2016). She was referencing the President's Commission on Critical Infrastructure Protection and its report that includes the term cyber security. As far as we found, this is the first official use of that term by the US Federal Government (President's Commission on Critical Infrastructure Protection, 1997).

We attempted to use Google Books' Ngram Viewer to find the first instance of cyber security in Google's English Corpus; however, it did not reliably map books to the correct published year. For example, the Ngram Viewer results indicate that a book published between 1952 and 1954 contains the term "cyber security" (Figure 3). The problem is that the books linked to this data are misdated, a known OCR issue in Google Books (Nunberg, 2009).

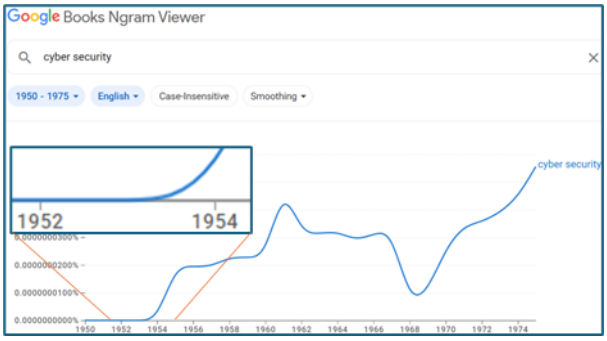


Figure 3: Google Books Ngram Viewer erroneously indicates the use of "cyber security" in books from the early 1950s.

Cyber Security or Cybersecurity

It is quite clear that the two-word form was initially more common, while the current trend is towards the single-word form [RQ2]. Google Trends' scores range from zero to 100 and do not represent absolute search volume. A line trending upwards means that a search term's popularity is increasing. Google Trends provides the following explanation:

> Numbers represent search interest relative to the highest point on the chart for the given region and time. A value of 100 is the peak popularity for the term. A value of 50 means that the term is half as popular. A score of 0 means there was not enough data for this term. (Google Trends, 2024)

In Figures 4 & 5, we show the Google Trends search results comparing "cybersecurity" to "cyber security" across the entire time period supported both worldwide and within the United States. Worldwide, the terms are converging, while it appears that the single-word form has overtaken the two-word form in US searches since roughly September 2024.

Figure 4: Google Trends results worldwide for "cyber security" (red – top line) vs. cybersecurity (blue), Jan 2004 – Jun 2025.

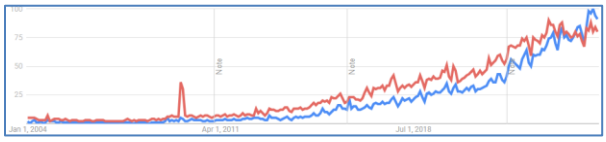


Figure 5: Google Trends results in the United States for "cyber security" (red) vs. cybersecurity (blue), Jan 2004 – Jun 2025.

Using the Google Books Ngram Viewer to compare instances of "cyber security" and "cybersecurity" across Google's English corpus of books published over the 20-year period 2002-2022, we see a much greater trend towards the single-word form of the word (Figure 6).

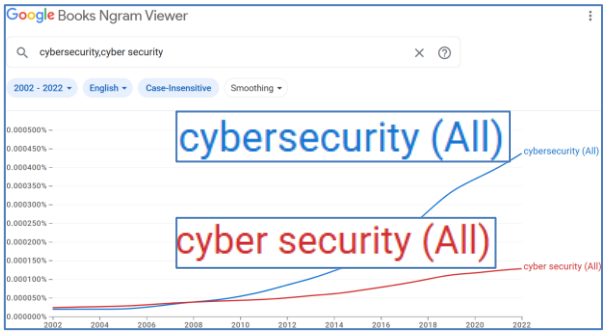


Figure 6: Google Books Ngram Viewer results for "cyber security" (red) vs. cybersecurity (blue), 2002 – 2022 (Google Books Ngram Viewer, 2025).

As acknowledged earlier, there are problems with the reliability of Google Books dating, but we consider this less of a concern given the sheer volume of instances of both word forms across time. The movement matches what we see in Google Trends, but to a greater extent, which seems understandable given that book writers are likely to be more deliberate in selecting their words than the general population submitting web searches.

A final indication of the single-word form gaining ascendancy is the results of our online dictionary definition search. All eight of the dictionaries referenced recognized our search for "cybersecurity" but only three (Merriam-Webster, OED, and WordWeb) recognized "cyber security" as a valid term and jumped to the cybersecurity definition page when searching for cyber security.

Definitions

Across the various sources, 60 definitions were collected per Table 1. All definitions are provided in Appendix B tables. Word frequency graphs are depicted in Appendix B figures.

Dictionaries (online)	8
Governmental & Standards Organizations	8
Tech companies	10
Cybersecurity companies	10
Academic papers	7
Universities	10
Generative AI	7

Table 1: Definition source and number of definitions collected.

In the following tables, we provide three representative definitions from each source group, followed by a brief analysis. Definitions from all sources are provided in tables in Appendix B.

Online Dictionaries
Cambridge Dictionary – "cybersecurity – things that are done to protect a person, organization, or country and their computer information against crime or attacks carried out using the internet" (Cambridge Dictionary, 2020)
Merriam Webster – "cybersecurity or cyber security – measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack" (Merriam Webster, 2019)
Dictionary.com – "cybersecurity or cyber security – 1. precautions taken to guard against crime that involves the internet, especially unauthorized access to computer systems and data connected to the internet. 2. the state of being protected against such crime." (Definition of Cybersecurity | Dictionary.com, n.d.)

Table 2: Three example definitions from online dictionaries.

The word frequency analysis of the collected dictionary definitions (see Table B-1, Figure B-1) shows that while no word was found across all eight dictionaries' definitions, the words *against*, *computer*, *internet*, *crime*, *system(s)*, and *attack(s)* were found in half or more. From these common words, it appears that online dictionaries most commonly define cybersecurity as the defense against internet-based attacks and crime.

Governmental & Standards Organizations
Congressional Research Service (CRS) – "Cybersecurity is a risk management process rather than an end-state. It involves continuous work to (1) identify and (2) protect against potential cybersecurity incidents; and to (3) detect; (4) respond to; and (5) recover from actual cybersecurity incidents" (Jaikaran, 2021)
Cybersecurity and Infrastructure Security Agency (CISA) – "Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information" (Cybersecurity and Infrastructure Security Agency, 2021)
NIST Glossary (cybersecurity) – "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" (National Institute of Standards and Technology, 2025b).

Table 3: Three example definitions from governmental and standards organizations.

The word frequency analysis of the collected definitions from governmental & standards organizations (see Table B-2, Figure B-2) shows that no word was found across all eight definitions. The words *information*, *cyber*, *communication(s)*, *cyberspace*, and *security* were found in half or more. Additionally, the words *risk*, *confidentiality*, *integrity*, and *availability* make a notable appearance, in contrast with the dictionary definitions. We infer from this word analysis that governmental & standards organizations take a broader, higher-level view of cybersecurity. Additionally, as *information* was the most common word, we conclude that the protection of information is central to these definitions.

Tech Companies
Microsoft – "Cybersecurity is a set of processes, best practices, and technology solutions that help you protect critical systems, data, and network from digital attacks." (Microsoft, n.d.)
Amazon – "Cybersecurity is the practice of safeguarding computers, networks, software applications, critical systems, and data from potential digital threats." (Amazon, n.d.)
Google – "Cybersecurity protects the data and integrity of computing assets belonging to or connecting to an organization's network. Its purpose is to defend those assets against all threat actors throughout the entire life cycle of a cyber attack." (Google, 2025)

Table 4: Three example definitions from tech companies.

The word frequency analysis of the tech companies' definitions (see Table B-3, Figure B-3) shows that no word appears in all 10 definitions. The words *systems*, *data*, *digital*, *practice(s)*, and *protect(ing)* were common to half or more. Other notable words include *network(s)*, *information*, and *application(s)*. In contrast to the previous two groups, tech companies' definitions

indicate concern about protecting data, networks, information, and applications.

Cybersecurity Companies
Palo Alto Networks – "Cybersecurity is the practice of protecting computers, servers, networks, devices, and sensitive data from malicious digital attacks and unauthorized access. It encompasses a comprehensive set of security measures, tools, and best practices to safeguard individual users and organizations from evolving cyber threats." (Palo Alto Networks, 2015)
CrowdStrike – "Cybersecurity is the act of defending digital assets, including networks, systems, computers and data, from cyberattacks." (Cranford, 2025)
Fortinet – "Cybersecurity is the combination of methods, processes, tools, and behaviors that protect computer systems, networks, and data from cyberattacks and unauthorized access. Although deeply rooted in technology, the effectiveness of cybersecurity also very much depends on people." (Fortinet, n.d.)

Table 5: Three example definitions from cybersecurity companies.

The word-frequency analysis of the cybersecurity companies' definitions (see Table B-4, Figure B-4) shows, for the first time, that a single word appears across all 10 definitions: *data*. The words *systems*, *networks*, *digital*, *unauthorized access*, *practice*, *threats*, and *protect* were common to half or more. Our analysis shows that cybersecurity companies view cybersecurity as a practice akin to the spirit of law or medicine, and they have a core concern with unauthorized access to data, systems, and networks.

Academic Papers
Craigen, Diakun-Thibault & Purse. Defining Cybersecurity – "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." (Craigen, Diakun-Thibault, & Purse, 2014, p. 14)
Schatz, Bashroush, & Wall. Towards a More Representative Definition of Cyber Security – "The approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users." (Schatz, 2017, p. 66)
Schiliro'. Towards a Contemporary Definition of Cybersecurity – "Cybersecurity is the collection and concerting of resources including personnel and infrastructure, structures, and processes to protect networks and cyber-enabled computer systems from events that compromise the integrity and interfere with property rights, resulting in some extent of the loss." (Schiliro', 2023, p. 2)

Table 6: Three example definitions from academic papers.

The word-frequency analysis of the academic papers' definitions (see Table B-5, Figure B-5) reveals no common word across all seven definitions. The words *cyber* and *security* were common to more than half. What's interesting is that most of the time, these words were not used as the term "cyber security." Our analysis indicates that academic definitions view cybersecurity as encompassing a wide array of aspects, suggesting the term's overall ambiguity and unsettled definition.

Universities
Harvard University – "Cybersecurity is a branch of computer science focused specifically on detecting, responding to, and preventing cyber attacks. It requires a high level of technical skills to understand computer systems, networks, and data privacy." (Harvard University, n.d.)
Stanford University – "Cybersecurity means prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation." (Stanford University, n.d.)
MIT – "Cybersecurity is defined as the practice of defending cyber infrastructures such as computers, servers, mobile devices, and IoT devices; as well as the data itself, from attack." (Massachusetts Institute of Technology, n.d.)

Table 7: Three example definitions from universities.

The word frequency analysis of the academic

institutions' definitions (see Table B-6, Figure B-6) finds no common word across all 10 definitions. The words *information*, *cyber*, *data*, *computer(s)*, and *system(s)* are common to at least half. The top word, information, seems to indicate a view of cybersecurity more in line with that of governmental and standards organizations, which are also concerned with information, rather than tech and cybersecurity companies, which are more concerned with data. Interestingly, within this group is the only repeated cybersecurity definition as the University of Cambridge directly uses one of the NIST definitions.

Generative AI
ChatGPT – "Cybersecurity is the practice of protecting systems, networks, and data from digital attacks, unauthorized access, and damage." (OpenAI, 2025.)
Microsoft CoPilot – "Cybersecurity is the practice of protecting systems, networks, and data from digital threats, such as cyberattacks, unauthorized access, and data breaches. It involves strategies, technologies, and best practices to ensure confidentiality, integrity, and availability of information. In short, it's the defense system for the digital world." (Microsoft, 2025.)
Google Gemini – "Cybersecurity is the practice of protecting systems, networks, and data from digital attacks." (Google, 2025.)

Table 8: Three example definitions from generative AI.

The word frequency analysis of the generative AIs' definitions (see Table B-7, Figure B-7) finds not one, but four common words across all seven definitions. Every generative AI definition we collected used *digital*, *systems*, *protecting*, and *networks*. As well, all but one referred to cybersecurity as a *practice*, were concerned with *unauthorized access*, and mentioned *data*. From this analysis, it appears that the LLMs are prioritizing cybersecurity company definitions over other sources when synthetically aggregating information to create a definition.

Word Frequency Analysis – All

Word frequency analysis across all 60 collected definitions reveals the top 30 words, as shown in Figure 7. The top 15 of these words are: *cybersecurity, protect(s,ing,ion), data, system(s), information, networks, cyber, security, practice(s), digital, technology(ies), unauthorized, computer, access, attacks.*

While there is a general consensus among the 60 collected definitions, no strong agreement exists on specific language [RQ3]. Drawing heavily on the definitions and evaluating the word-frequency analysis of all 60, we might synthesize a current, common definition of cybersecurity as *the practice of protecting digital data, computer systems, information technology, and networks against attacks, threats, and unauthorized access*.

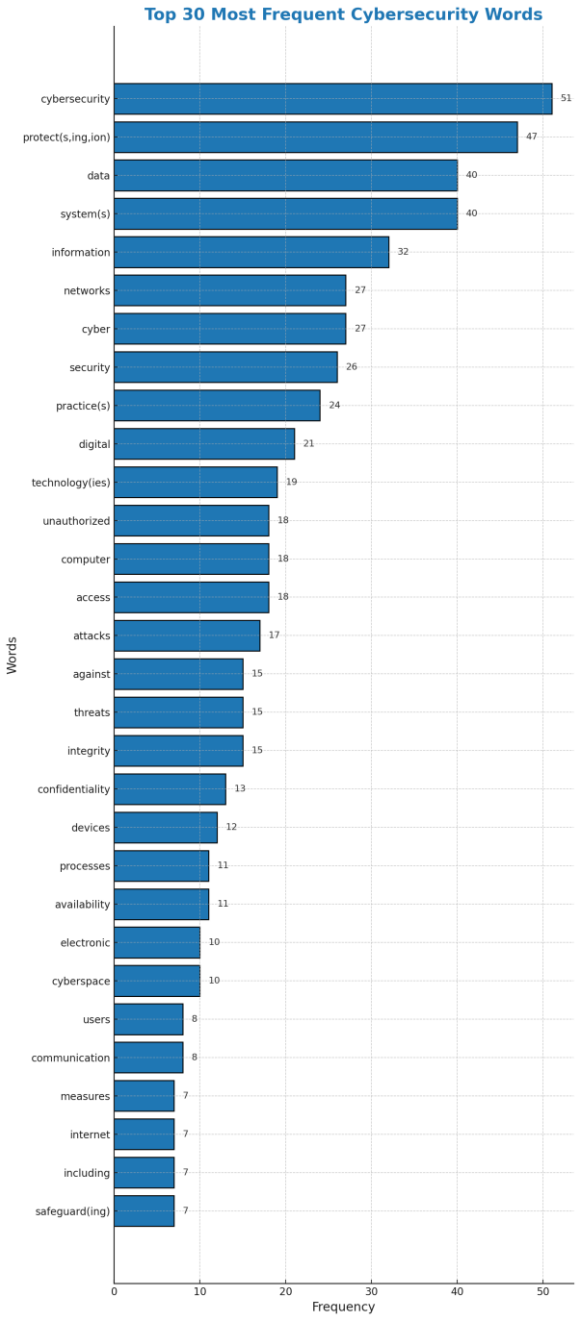


Figure 7: Top 30 words among our 60 collected definitions

5. CONCLUSION & FUTURE WORK

Reflecting on computer science, Alan Perlis wrote, "In trying to define our field I sometimes feel that we are too impatient, are in too much of a rush, to establish the core" (Perlis, n.d., p. 3). We approached this investigation of the term cybersecurity with patience, tracing its first verified use to Kaduna Memories (McKinney, 1990), noting the shift in preference from the two-word form, cyber security, to the one-word form, cybersecurity, and analyzing definitions across government, academia, and industry. Some are likely frustrated that cybersecurity does not yet have a more widely accepted definition; however, the history of computer science suggests it takes time to flesh things out. We took what we found and synthesized a definition for cybersecurity as *the practice of protecting digital data, computer systems, information technology, and networks against attacks, threats, and unauthorized access*.

While that captures the current state of things, it seems clear that our collective understanding is still evolving and will likely not be settled soon. Notably, the word risk appears in none of the top 15 most frequent words across our 60 collected definitions (see Figure 8), despite the panelist quoted in our introduction defining cybersecurity in explicitly risk-based terms — "the application of risk management to digital assets." This gap between formal definitions and how practitioners describe the field in practice suggests risk, and related terms like analysis and management, may be poised to gain more prominent representation in cybersecurity definitions as the field continues to mature.

Future research should explore how these definitional differences shape policy, education, and the global cybersecurity workforce. As technology advances, the term itself may continue to evolve or be replaced.

6. REFERENCES

Alexei, L. A., & Alexei, A. (2022). The difference between cyber security vs information security. Journal of Engineering Science, (4), 72-83. https://doi.org/10.52326/jes.utm.2022.29(4).08

Amazon. (n.d.). What is Cybersecurity? - Cybersecurity Explained - AWS. Amazon Web Services, Inc. https://aws.amazon.com/what-is/cybersecurity/

Akamai. (n.d.). What Is Cybersecurity or Cyber Security? Akamai. Retrieved June 17, 2025, from https://www.akamai.com/glossary/what-is-cybersecurity

AMD. (n.d.). AMD Design Security Technology. AMD. Retrieved June 17, 2025, from https://www.amd.com/zh-cn/products/adaptive-socs-and-fpgas/technologies/design-security.html?

Bay, M. (2016). What is cybersecurity. French Journal for Media Research, 6, 1-28. https://www.researchgate.net/profile/Morten-Bay/publication/308609163_WHAT_IS_CYBERSECURITY_In_search_of_an_encompassing_definition_for_the_post-Snowden_era/links/673666db69c07a411447404e/WHAT-IS-CYBERSECURITY-In-search-of-an-encompassing-definition-for-the-post-Snowden-era.pdf

Burley, D.L., Bishop, M., Buck, S., Ekstrom, J.J., Futcher, L., Gibson, D., Hawthorne, E.K., Kaza, S., Levy, Y., Mattord, H., & Parrish, A. (2017, December 31). Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf

Broadcom. (n.d.). Broadcom Inc. | What is Cybersecurity? Broadcom.com. Retrieved June 17, 2025, from https://www.broadcom.com/topics/cybersecurity

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Analysis, 42(8), 1643-1669. https://doi.org/10.1111/risa.13687

Cambridge Dictionary. (2020, February 5). CYBERSECURITY | meaning in the Cambridge English Dictionary. Cambridge.org. https://dictionary.cambridge.org/dictionary/english/cybersecurity

Canongia, C. & Mandarino, R. (2014). Cybersecurity: The New Challenge of the Information Society. In I. Management Association (Ed.), Crisis Management: Concepts, Methodologies, Tools, and Applications (pp. 60-80). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-4666-4707-7.ch003

Carnegie Mellon University. (n.d.). Cybersecurity and privacy. CyLab Security and Privacy Institute. https://www.cmu.edu/iso/aware/presentation/sec101-idtheft.pdf

Cisco. (n.d.). What is cybersecurity? Cisco.

https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html

Claude. (2025). ClaudeAI [Large language model]. Response to "what is the best general concise definition of cybersecurity"

Cloudflare. (n.d.). What is cyber security? Cloudflare.com. https://www.cloudflare.com/learning/security/what-is-cyber-security/

Companies Marketcap. (n.d.) Largest tech companies by market cap. Retrieved August 15, 2025, from https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap

Computer Science Is Not About Computers, Any More Than Astronomy Is About Telescopes – Quote Investigator. (n.d.). https://quoteinvestigator.com/2021/04/02/computer-science/

Copilot. (2025). Response to "Who first used the term cyber security or cybersecurity?". Microsoft. Retrieved June 5, 2025.

Chang, E. S., Jain, A. K., Slade, D. M., & Tsao, S. L. (1999). Managing cyber security vulnerabilities in large networks. Bell Labs Technical Journal, 4(4), 252–272. https://doi.org/10.1002/bltj.2202

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology innovation management review, 4(10). https://www.timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf

Cranford, J. (2025, January 17). What is IT Security? Information Technology Security | CrowdStrike. Crowdstrike.com. https://www.crowdstrike.com/en-us/cybersecurity-101/cybersecurity/it-security/?

Cybersecurity, n. meanings, etymology and more | Oxford English Dictionary. (2023). Oed.com. https://doi.org/10.1093//OED//6503222281

Cybersecurity - Wiktionary, the free dictionary. (2022). Wiktionary. https://en.wiktionary.org/wiki/cybersecurity

Cybersecurity- WordWeb dictionary definition. (2025). Wordwebonline.com. https://www.wordwebonline.com/en/CYBERSECURITY

Cybersecurity and Infrastructure Security Agency. (2021, February 1). What is Cybersecurity? https://www.cisa.gov/news-events/news/what-cybersecurity

"Cybersecurity: The Future of Financial Security." SAP, www.sap.com/products/financial-management/what-is-cybersecurity.html.

Definition of cybersecurity. (2025, June 2). Collinsdictionary.com; HarperCollins Publishers Ltd. https://www.collinsdictionary.com/dictionary/english/cybersecurity

Definition of cybersecurity | Dictionary.com. (n.d.). www.dictionary.com. https://www.dictionary.com/browse/cybersecurity

DeepSeek. (2025). DeepSeek [Large language model]. Response to "what is the best general concise definition of cybersecurity"

Denning, P. J. (2008). The computing field: Structure. https://calhoun.nps.edu/server/api/core/bitstreams/987c402d-d661-45d0-8c13-40ce573cd394/content

EduRank. (2025, March 2). World's 100+ best cyber security universities [rankings]. EduRank.org - Discover university rankings by location. https://edurank.org/cs/cybersecurity/

European Union Agency for Cybersecurity. (2015, December). Definition of cybersecurity, gaps and overlaps in standardization V1. https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity_Definition_Gaps_v1_0.pdf

European Union Agency for Cybersecurity. (2017, September). ENISA overview of cybersecurity and related terminology V1. https://www.enisa.europa.eu/sites/default/files/all_files/2017-09-07-ENISAoverviewOfCybersecurityAndRelatedTechnology.pdf

F5. (n.d.). What Is Cybersecurity? F5, Inc. https://www.f5.com/glossary/cybersecurity

Fortinet. (n.d.). What Is Cybersecurity? Definition & Types. Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-cybersecurity

Fox, R. (1997). News track. Commun. ACM 40, 12 (Dec. 1997), 9–10. https://doi.org/10.1145/265563.265564

Frye, J. (2000), CIO Cyber Security Notes. https://www.nist.gov/publications/cio-cyber-security-notes

Furnell, S., & Collins, E. (2021). Cyber security: What are we talking about? Computer Fraud & Security, 2021(7), 6–11. https://doi.org/10.1016/S1361-3723(21)00073-7

Georgia Institute of Technology. (n.d.). Georgia Tech Cybersecurity. https://www.cyber.

gatech.edu

Gest, E. (1995, August 20). The jobs of the past, the jobs of the future. Los Angeles Times. https://www.proquest.com/hnplatimes/docview/2030684086/fulltextPDF/C2E46758D7744C30PQ/1?accountid=14606&sourcetype=Historical%20Newspapers

Gibson, W. (1984). Neuromancer. Ace Books. https://archive.org/details/neuromancer_202209/page/n3/mode/2up?q=cyberspace

Gologanoff, C. (2023, August 4). Cybersecurity: Then and Now. https://fuel.reyrey.com/it-and-networking/2023/08/cybersecurity-then-and-now/

Google. (2025). Google Search [Large language model]. Response to "who first coined the term cybersecurity"

Google. (2025). Gemini [Large language model]. Response to "what is the best general concise definition of cybersecurity"

Google Books Ngram Viewer. (2025). Google.com. https://books.google.com/ngrams/graph?content=cyber+security%2Ccybersecurity&year_start=2002&year_end=2022&corpus=en

Google Trends. (2024). Google.com. https://trends.google.com/trends/explore?q=cybersecurity

Google. (2025). What is cybersecurity? Google Cloud. https://cloud.google.com/security/resources/insights/what-is-cyber-security

Hanson, C. & Zipp, Y. (1996, July 18). News In Brief. The Christian Science Monitor. https://www.csmonitor.com/1996/0718/071896.news.news.1.html

Harvard University. (n.d.). Cybersecurity. Belfer Center for Science and International Affairs. https://extension.harvard.edu/blog/cybersecurity-vs-software-engineering-which-is-right-for-you/

Husick, L. A., Arkfeld, M. R., Vandagriff, D. P., & Flax, J. M. (July 1995). Winning the Information Revolution. ABA Journal. Vol. 81, No. 7, pp. 62-67. https://www.jstor.org/stable/27835870?seq=1

International Organization for Standardization. (2023). Cybersecurity - guidelines for internet security (ISO/IEC 27032:2023). https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-2:v1:en

International Organization for Standardization. (2012). Information technology - security techniques - guidelines for cybersecurity (ISO/IEC 27032:2012). https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

Jaikaran, C. (2021, September 29). Federal cybersecurity: background and issues for congress (CRS Report No. R46926) https://www.congress.gov/crs-product/R46926

Jamie Gorelick Discusses the Birth of Cybersecurity. (2016, July 14). Wilmerhale.com. https://www.wilmerhale.com/en/insights/news/2016-07-14-jamie-gorelick-discusses-the-birth-of-cybersecurity

Kinsella, D. (2022, July 7). What's in a Name? The Origin of Cyber. CISO Global. https://www.ciso.inc/blog-posts/origin-cyber/

Koch, W. (1994, April 10). The Card is in the Future of Medicine. The Dispatch-Argus (Moline, IL). Available from NewsBank: Access World News – Historical and Current: https://infoweb-newsbank-com.liblink.uncw.edu/apps/news/document-view?p=WORLDNEWS&docref=news/16A174BD85245478

Lal, A. (2023, August 14). Council Post: The Evolution of Cybersecurity and How Businesses Can Prepare for the Future. Forbes. https://www.forbes.com/councils/forbesbusinesscouncil/2023/08/14/the-evolution-of-cybersecurity-and-how-businesses-can-prepare-for-the-future/

Lardner, G. (1997, September 6). Panel urges US to power up cyber security. Washington Post. https://www.proquest.com/hnpwashingtonpost/docview/1458147166/fulltextPDF/DDE121A1802D4C42PQ/1?accountid=14606&sourcetype=Newspapers

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Lindemulder, G., Kosinski, M., & Jonker, A. (2025, June 13). What is cybersecurity? IBM. https://www.ibm.com/think/topics/cybersecurity

Merriam Webster. (2019). Definition of CYBERSECURITY. Merriam-Webster.com. https://www.merriam-webster.com/dictionary/cybersecurity

Massachusetts Institute of Technology. (n.d.). Cybersecurity at MIT Sloan (CAMS). https://innovation.mit.edu/assets/Enhancing

-Cybersecurity-The-Role-of-Innovation-Ecosystems.pdf

McKinney, J. (1990). Kaduna Memories. Del Rey.

Meta AI. (2025). Meta AI [Large language model]. Response to "what is the best general concise definition of cybersecurity"

Microsoft. (n.d.). What is Cybersecurity? Microsoft Security. Www.microsoft.com. https://www.microsoft.com/en-us/security/business/security-101/what-is-cybersecurity

Microsoft. (2025). CoPilot [Large language model]. Response to "what is the best general concise definition of cybersecurity"

National Institute of Standards and Technology. (2025, May). Cyber Security. https://csrc.nist.gov/glossary/term/cyber_security

National Institute of Standards and Technology. (2025, May). cybersecurity. https://csrc.nist.gov/glossary/term/cybersecurity

Neil, L., Haney, J. M., Buchanan, K., & Healy, C. (2023). Analyzing cybersecurity definitions for non-experts. In S. Furnell & N. Clarke (Eds.), Human aspects of information security and assurance (Vol. 674, pp. 391-404). Springer. https://doi.org/10.1007/978-3-031-38530-8_31

Newell, A., Perlis, A. J., & Simon, H. A. (1967). What is Computer Science. Science, 157, 1373–1374. https://iiif.library.cmu.edu/file/Newell_box00048_fld04157_doc0005/Newell_box00048_fld04157_doc0005.pdf

New York University. (n.d.). Cybersecurity and Privacy. Tandon School of Engineering. https://engineering.nyu.edu/academics/programs/cybersecurity-ms/cybersecurity-and-privacy

New York University. (n.d.). NYU Cyber Fellows. https://engineering.nyu.edu/academics/programs/cybersecurity-ms-online

North Carolina Partnership for Cybersecurity Excellence. (2025, April). 4th Annual NC Cybersecurity Symposium Agenda. https://www.nc-pace.org/_files/ugd/9041bd_827b1742196f43c78147622bbc5457c6.pdf

Nunberg, G. (2009). Language Log. Google Books: A Metadata Train Wreck. https://languagelog.ldc.upenn.edu/nll/?p=1701

Okta. (2024, August 31). What Is Cybersecurity? Definition, Threats & More. Www.okta.com. https://www.okta.com/identity-101/cybersecurity/

OpenAI. (2025). ChatGPT [Large language model]. Response to "what is the best general concise definition of cybersecurity"

Palo Alto Networks. (2015). What Is Cybersecurity? Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security?

Perlis, A. J. (n.d.). What is Computer Science, again. https://stacks.stanford.edu/file/druid:db941ss9825/db941ss9825.pdf

Perplexity. (2025). Perplexity [Large language model]. Response to "what is the best general concise definition of cybersecurity"

President's Commission on Critical Infrastructure Protection. (1997, October). Critical Foundations, Protecting America's Infrastructures. https://sgp.fas.org/library/pccip.pdf

Risen, J. (1999, May 12). Energy secretary outlines plan to improve nuclear security. The New York Times. https://www.nytimes.com/1999/05/12/world/energy-secretary-outlines-plan-to-improve-nuclear-security.html

Salesforce. (n.d.). What is Cybersecurity? Your Guide to Digital Defense. Salesforce. Retrieved June 17, 2025, from https://www.salesforce.com/platform/data-security/what-is-cybersecurity/#wic

SailPoint. (2025, April 6). Types of cybersecurity. SailPoint. https://www.sailpoint.com/identity-library/five-types-of-cybersecurity

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. Journal of Digital Forensics, Security and Law, 12(2), 8. https://commons.erau.edu/cgi/viewcontent.cgi?article=1476&context=jdfsl

Schiliro', F. (2023). Towards a contemporary definition of cybersecurity. arXiv. https://arxiv.org/pdf/2302.02274.pdf

SentinelOne. (2025, March 28). What is Cyber Security? Types, Importance & Threats. SentinelOne. https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-cyber-security/

ServiceNow. (2025). What is Cyber Security? ServiceNow. https://www.servicenow.com/products/security-operations/what-is-cyber-security.html

Simons, J. (1997, October 21). U.S. vulnerability

on cyber-security, is cited by report. Wall Street Journal. https://www.proquest.com/hnpwallstreetjournal/docview/1620006534/fulltextPDF/B553430C6B4A4A01PQ/1?accountid=14606&sourcetype=Newspapers

Siudak, R. (2022). Cybersecurity discourses and their policy implications. Journal of Cyber Policy, 7(3), 318–335. https://doi.org/10.1080/23738871.2023.2167607

Stanford University. (n.d.). Cyber policy. Freeman Spogli Institute. https://fsi.stanford.edu/news/where-new-national-cybersecurity-strategy-differs-past-practice

Tribune News Services. (1999, May 23). NASA computers found vulnerable to hackers. Chicago Tribune. https://www.proquest.com/hnpchicagotribune/docview/2293518556/fulltextPDF/6BE783547E274E6FPQ/1?accountid=14606&sourcetype=Historical%20Newspapers

University of California, Berkeley. (n.d.). What is Cybersecurity? UC Berkeley School of Information. https://ischoolonline.berkeley.edu/cybersecurity/what-is-cybersecurity/

University of Cambridge. (n.d.). Glossary of Terms – Cybersecurity. University Information Services. https://help.uis.cam.ac.uk/service/security/terms#cybersecurity

University of Illinois Urbana-Champaign. (n.d.). *Information technology security policy (INFOSEC)*. Illinois Cybersecurity Scholars Program. https://cybersecurity.illinois.edu/illinois-security-program/

University of Texas at Austin. (n.d.). Center for Identity – Cybersecurity. https://security.utexas.edu/policies/irusp

Urban Dictionary: cybersecurity. (2015). Urban Dictionary. https://www.urbandictionary.com/define.php?term=cybersecurity

Zscaler. (n.d.). What Is Cybersecurity? Zscaler.com; Zscaler, Inc. Retrieved June 17, 2025, from https://www.zscaler.com/resources/security-terms-glossary/what-is-cybersecurity

APPENDIX A

First Use of the Term Cyber Security

This table is sorted by date of the cited source. Items at the top are older than those at the bottom.

Kaduna Memories June 13, 1990	"Bové glanced at his boss for a reaction. 'You're gonna love this: Turns out the guy used to work **cyber security** for us downside. A technopath. Used to make sure SPARTOS was up on his inoculations.' SPARTOS was the Virtual Network AI in charge of OLD security." (McKinney, 1990)
The Dispatch-Argus April 10, 1994	"Currently, state laws guard the privacy of medical records. But their vast differences raise questions for **cyber security**" (Koch, 1994).
ABA Journal July 1995	"**Cyber-Security**. While loping down that ol' information superhighway, you ought to keep in mind that bandits come with the territory" (Husick et al., 1995, p. 67).
Los Angeles Times August 20, 1995	"There have already been some well-publicized cases involving the new demands of **cyber security**, such as that of computer security expert Tstutomo [sic] Shimomura, who helped nail hacker Kevin Mitnick" (Gest, 1995, p. SM26).
Christian Science Monitor July 18, 1996	"The US needs the equivalent of the "Manhattan Project" - which developed the first atom bomb - for **cyber security**, the Clinton administration said" (Hanson & Zipp, 1996).
Washington Post September 6, 1997	"Panel Urges U.S. to Power Up **Cyber Security**" (Lardner, 1997, p. A3)
President's Commission on Critical Infrastructure Protection October 1997	"Their risk analysis weighs the cost of physical and cyber disruption against the cost of physical and **cyber security**."

	(President's Commission on Critical Infrastructure Protection, 1997, p. 27)
Wall Street Journal October 21, 1997	"U.S. Vulnerability on **Cyber-Security**, Is Cited by Report" (Simons, 1997, p. B6).
ACM Digital Library December 1997	"The commission's study of U.S. telecommunications systems, electric-power grids, transportation, oil and gas delivery, storage structures, water systems, emergency services, and government services recommended quadrupling the federal amount spent on **cyber-security** research to $1 billion during the next seven years" (Fox, 1997, p. 9).
New York Times May 12, 1999	"The new 'security czar' will be a senior official who will report directly to Mr. Richardson and will oversee all security-related functions, including offices handling **cyber-security**, nuclear material control and background checks on foreign visitors to the labs" (Risen, 1999).
Chicago Tribune May 23, 1999	"A government investigation into NASA's **cyber security** found it so vulnerable to attack that hackers could easily disrupt command and control operations, including the tracking of Earth-orbiting spacecraft" (Tribune News Services, 1999, p. C13).
IEEE Xplore October-December 1999	"Managing **Cyber Security** Vulnerabilities in Large Networks" (Chang et al., 1999)
NIST publications July 19, 2000	"CIO **Cyber Security** Notes" (Frye, 2000).

Table A-1: Earliest evidence of the use of the term cyber security from a variety of sources.

APPENDIX B

Cybersecurity Definitions

The following online dictionary definitions are ordered alphabetically by the dictionary name.

Online Dictionaries – Cybersecurity Definitions	
Cambridge Dictionary	"cybersecurity – things that are done to protect a person, organization, or country and their computer information against crime or attacks carried out using the internet" (Cambridge Dictionary, 2020)
Collins Dictionary	"cybersecurity - the state of being safe from electronic crime and the measures taken to achieve this" (Definition of Cybersecurity, 2025)
Dictionary.com	"cybersecurity or cyber security – 1. precautions taken to guard against crime that involves the internet, especially unauthorized access to computer systems and data connected to the internet. 2. the state of being protected against such crime." (Definition of Cybersecurity | Dictionary.com, n.d.)
Merriam-Webster	"cybersecurity or cyber security – measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack" (Merriam Webster, 2019)
Oxford English Dictionary	"cybersecurity – security relating to computer systems or the internet, esp. that intended to protect against viruses or fraud" ("Cybersecurity, N. Meanings, Etymology and More | Oxford English Dictionary," 2023).
Urban Dictionary	"Cybersecurity is system of computer technology that protects and integrates global interconnected information technology infrastructure" (Urban Dictionary: Cybersecurity, 2015). "The illusion of preventing human mistakes by technical means"
Wiktionary	"cybersecurity – security against electronic attacks such as cyberwarfare or cyberterrorism" (Cybersecurity - Wiktionary, the Free Dictionary, 2025).
WordWeb Online	"cybersecurity – (computing) security against electronic attack or spying" (Cybersecurity- WordWeb Dictionary Definition, 2025)

Table B-1: Online dictionary definitions for cybersecurity.

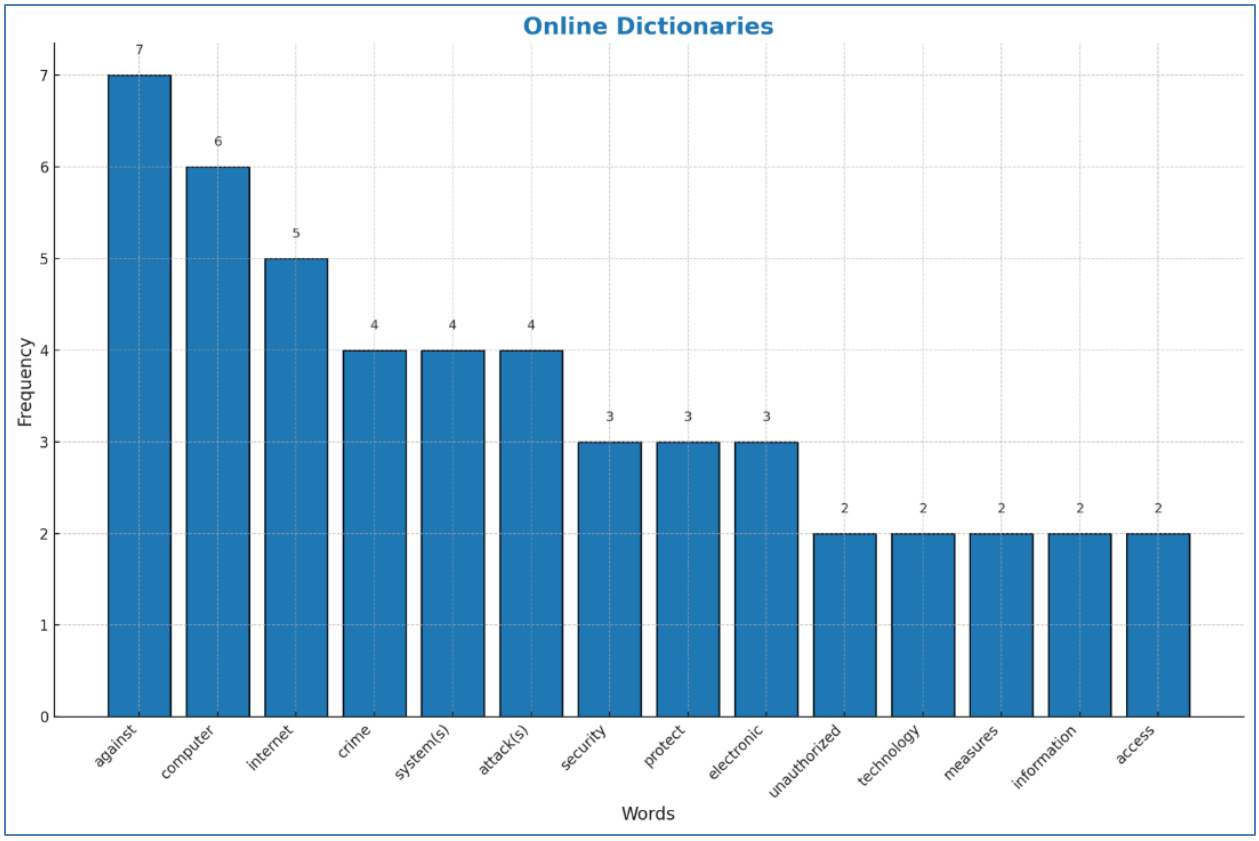


Figure B-1: Online dictionary word frequency bar graph

The following governmental / standards organizations' definitions are ordered alphabetically by the organization name.

Governmental / Standards Organizations – Cybersecurity Definitions	
Congressional Research Service (CRS)	"Cybersecurity is a risk management process rather than an end-state. It involves continuous work to (1) identify and (2) protect against potential cybersecurity incidents; and to (3) detect; (4) respond to; and (5) recover from actual cybersecurity incidents" (Jaikaran, 2021)
Cybersecurity and Infrastructure Security Agency (CISA)	"Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information" (Cybersecurity and Infrastructure Security Agency, 2021)
European Union Agency for Cybersecurity (ENISA – formerly European Union Agency for Network and Information Security)	"Cybersecurity comprises all activities necessary to protect cyberspace, its users, and impacted persons from cyber threats" (European Union Agency for Cybersecurity, 2017, p. 6).
International Organization for Standardization (ISO) 2023	"safeguarding of people, society, organizations and nations from cyber risks; Note 1 to entry: Safeguarding means to keep cyber risk at a tolerable level" (International Organization for Standardization, 2023)
ISO 2012	"Cyberspace security. preservation of confidentiality, integrity and availability of information in the Cyberspace; Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved; Note 2 to entry: Adapted from the definition for information security in ISO/IEC 27000:2009" (International Organization for

	Standardization, 2012)
Joint Task Force (JTF) on Cybersecurity Education; collaboration among: Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers Computer Society (IEEE CS), Association for Information Systems Special Interest Group on Security (AIS SIGSEC), International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)	"A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management" (Burley et al., 2017, p. 16)
National Institute of Standards and Technology (NIST) Glossary – cyber security	"The ability to protect or defend the use of cyberspace from cyber attacks" (National Institute of Standards and Technology, 2025a).
NIST Glossary – cybersecurity	"Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" (National Institute of Standards and Technology, 2025b).

Table B-2: Governmental and standards organizations' definitions for cybersecurity.

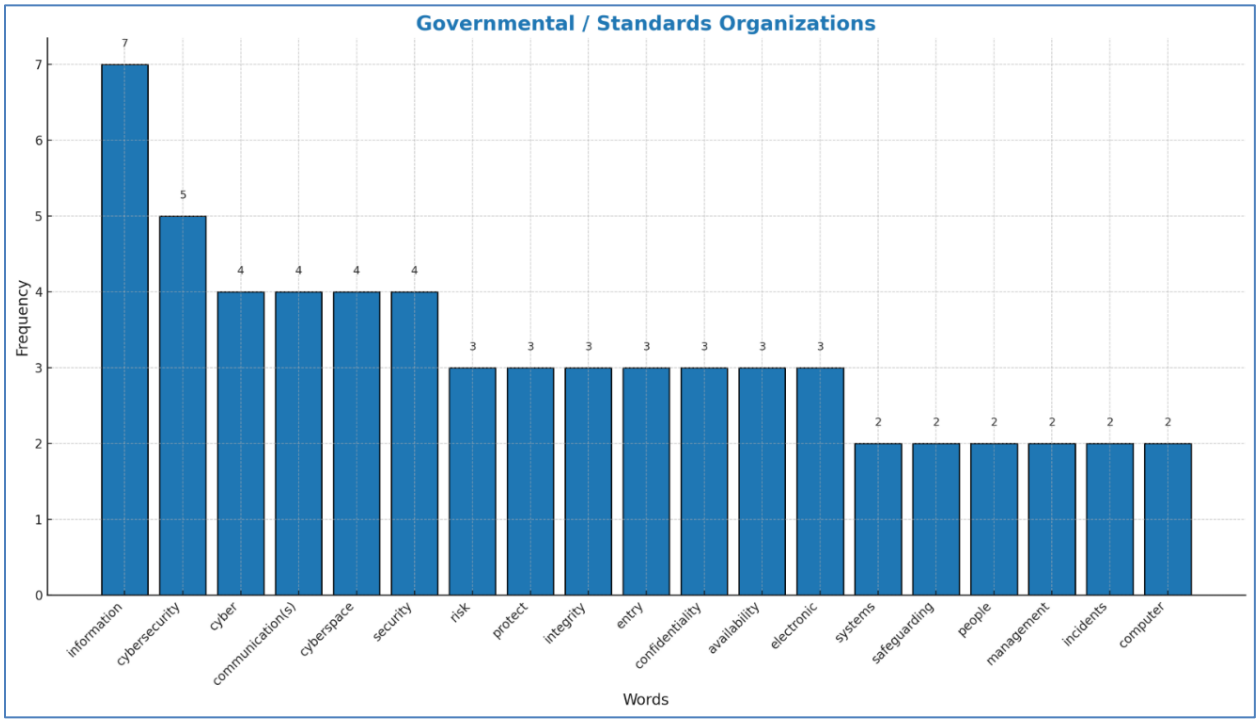


Figure B-2: Governmental / standards organizations word frequency bar graph

The following tech companies' definitions are ordered by company market cap.

Tech Companies – Cybersecurity Definitions	
Microsoft	"Cybersecurity is a set of processes, best practices, and technology solutions that help you protect critical systems, data, and network from digital attacks." (Microsoft, n.d.)
Google	"Cybersecurity protects the data and integrity of computing assets belonging to or connecting to an organization's network. Its purpose is to defend those assets against all threat actors throughout the entire life cycle of a cyber attack." (Google, 2025)
Amazon	"Cybersecurity is the practice of safeguarding computers, networks, software applications, critical systems, and data from potential digital threats." (Amazon, n.d.)
Broadcom	"Cybersecurity refers to any method used to protect computer systems, networks and programs from digital attacks. The increasing reliance on digital technologies and the interconnected nature of the internet, has made cybersecurity a critical factor in ensuring the confidentiality and integrity of information." (Broadcom, n.d.)
SAP	"Cybersecurity is the practice of protecting networks, devices, applications, systems, and data from cyberthreats." ("Cybersecurity: The Future of Financial Security")
AMD	"Cybersecurity focuses on protecting information in cyberspace. Therefore, in most application scenarios, cybersecurity is essentially a subset of information assurance." (AMD, n.d.)
Cisco	"Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users through ransomware; or interrupting normal business processes." (Cisco, n.d.)
Salesforce	"Cybersecurity is an organization's defense against the constant ambush of digital threats. It serves as a shield against online criminals, manipulation, and deceit from both internal and external threats." (Salesforce, n.d.)
IBM	"Cybersecurity refers to any technologies, practices and policies for preventing cyberattacks or mitigating their impact. Cybersecurity aims to protect computer systems, applications, devices, data, financial assets and people against ransomware and other malware, phishing scams, data theft and other cyberthreats." (Lindemulder et al., 2025)
ServiceNow	"Cyber security describes the policies, tools, and roles associated with defending computer systems and data from unauthorized access or disruption." (ServiceNow, 2025)

Table B-3: Tech company definitions for cybersecurity.

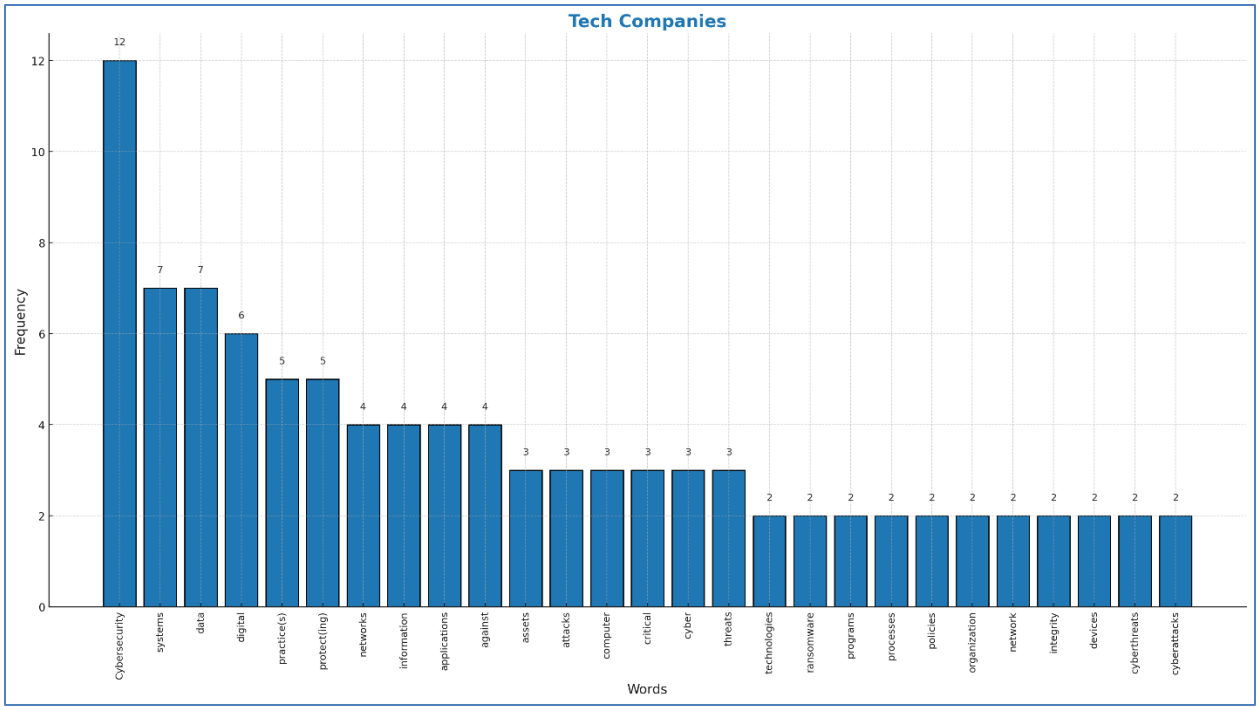


Figure B-3: Tech companies' word frequency bar graph

The following cybersecurity companies' definitions are ordered by company market cap.

Cybersecurity Companies – Cybersecurity Definitions	
Palo Alto Networks	"Cybersecurity is the practice of protecting computers, servers, networks, devices, and sensitive data from malicious digital attacks and unauthorized access. It encompasses a comprehensive set of security measures, tools, and best practices to safeguard individual users and organizations from evolving cyber threats." (Palo Alto Networks, 2015)
CrowdStrike	"Cybersecurity is the act of defending digital assets, including networks, systems, computers and data, from cyberattacks." (Cranford, 2025)
Fortinet	"Cybersecurity is the combination of methods, processes, tools, and behaviors that protect computer systems, networks, and data from cyberattacks and unauthorized access. Although deeply rooted in technology, the effectiveness of cybersecurity also very much depends on people." (Fortinet, n.d.)
Cloudflare	"Cyber security is the practice of protecting networks, applications, confidential or sensitive data, and users from cyber attacks." (Cloudflare, n.d.)
Zscaler	"Cybersecurity is the state of being protected in cyberspace, including measures taken to protect computer systems against unauthorized access or attack. It refers to the policies, processes, and technologies to protect networks, devices, and data from cybercrime and data breaches. Today, at an enterprise level, cybersecurity is typically carried out through a security program, including continual risk assessment to see where an organization could be vulnerable." (Zscaler, n.d.)
Okta	"Cybersecurity, also known as information technology (IT) security, is the method of keeping digital systems and information safe from potential threats. Cybersecurity models often include layers of protection involving multiple domains. Cyber threats can come from inside or outside of an organization. As such, cybersecurity measures should be comprehensive and multifaceted. Cybersecurity needs to protect networks, devices, data, and communications from access to unauthorized users. It should strive to guarantee confidentiality and privacy, data integrity, and the availability of data when authorized." (Okta, 2024)

F5	"Cybersecurity is the practice of protecting computer systems, networks, applications, and data from digital threats, malicious attacks, and unauthorized access. It encompasses a range of strategies, technologies, and processes designed to safeguard digital environments from evolving cyber risks." (F5, n.d.)
Akamai	"Cybersecurity is the practice of protecting IT (information technology) networks, systems, data, applications, and devices from attacks. Cyberattacks are typically designed to disrupt business operations, gain unauthorized access to systems, take data or intellectual property, or steal or extort money from organizations. Strong cybersecurity requires a multilayered defense involving technologies, processes, policy, and security expertise to protect organizations from attacks that can result in loss of business and reputation." (Akamai, n.d.)
SailPoint	"Cybersecurity is the practice of using technology, controls, and processes to protect digital networks, devices, and data from unauthorized access by malicious attackers or unintentional activity. It protects the confidentiality, integrity, and availability of information." (SailPoint, 2025)
SentinelOne	"Cybersecurity is the practice of protecting internet-connected systems of hardware, software, and data, from cyber threats. These threats range from ransomware and data theft to phishing scams. Cybersecurity encompasses everything from keeping sensitive information safe to making sure IT systems work properly." (SentinelOne, 2025)

Table B-4: Cybersecurity company definitions for cybersecurity.

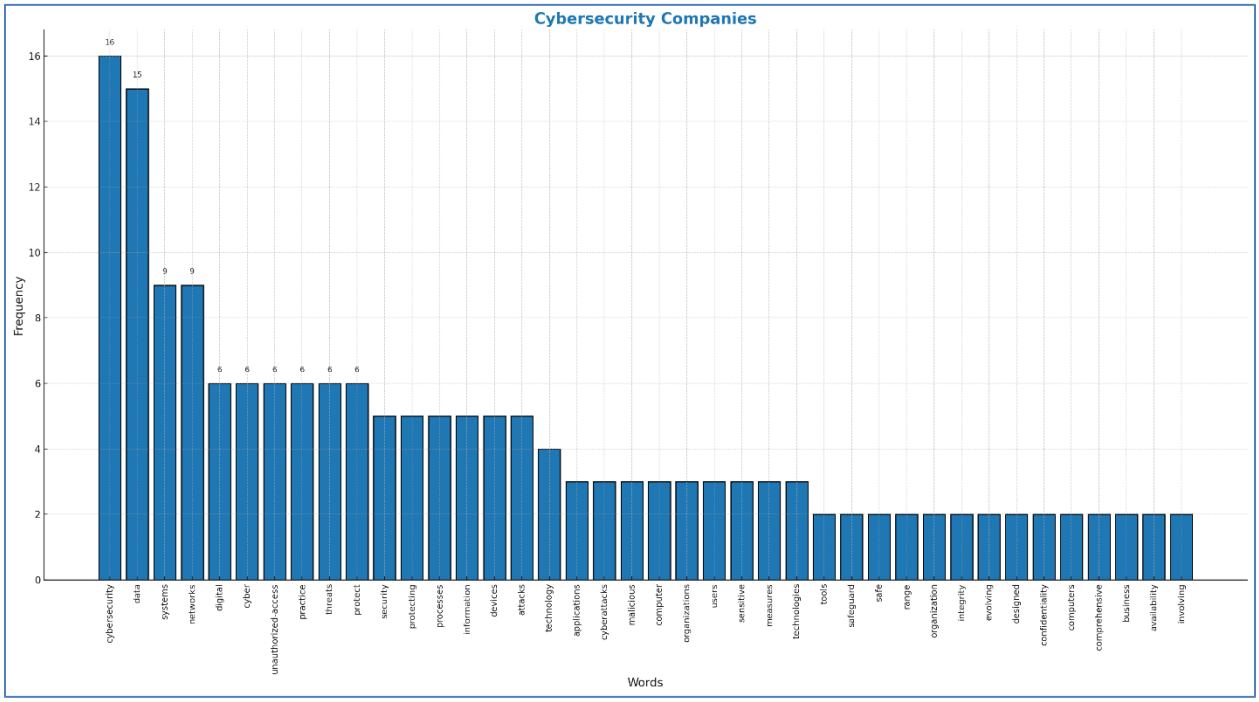


Figure B-4: Cybersecurity companies' word frequency bar graph.

The following academic paper definitions are ordered by publishing year.

Academic Papers – Cybersecurity Definitions	
Canongia & Mandarino (2014) Cybersecurity: The New Challenge of the Information Society	"The art of ensuring the existence and continuity of the Information Society of a nation, guaranteeing and protecting, in Cyberspace, its information assets and critical infrastructure." (Canongia & Mandarino, 2014)

Craigen, Diakun-Thibault & Purse (2014) Defining Cybersecurity	"Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." (Craigen, Diakun-Thibault, & Purse, 2014, p. 14)
Schatz, Bashroush, & Wall (2017) Towards a More Representative Definition of Cyber Security	"The approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users." (Schatz, 2017, p. 66)
Li & Liu (2021) A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments	"Cyber-security includes practical measures to protect information, networks and data against internal or external threats." (Li & Liu, 2021, p. 8181)
Alexei & Alexei (2022) The Difference between Cyber Security vs. Information Security	"From the definitions presented above, it can be concluded that cyber security is an umbrella term, which includes several types of security, the common property of which is the connection to communication networks, the services provided to users are electronic services because cyber security does not exist outside cyberspace." (Alexei & Alexei, 2022, p. 78)
Cains, Flora, Taber, King & Henshel (2022) Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation	"Cybersecurity is the iterative process of maintaining quantifiable levels of cyber system dependability and control over verifiable data provenance, confidentiality, integrity, and accessibility (CIA) via comprehensive system awareness, human factor and effects characterization, resource protection and management, accurate intrusion detection, threat prediction and prevention, resilient system functionality, and systemic solutions in a cost-limited environment of socio-technical interactions between diverse dimensions and factors, despite evolving security standards and variations in security competence." (Cains, et al., 2022, p. 1648)
Schiliro' (2023) Towards a Contemporary Definition of Cybersecurity	"Cybersecurity is the collection and concerting of resources including personnel and infrastructure, structures, and processes to protect networks and cyber-enabled computer systems from events that compromise the integrity and interfere with property rights, resulting in some extent of the loss." (Schiliro', 2023, p. 2)

Table B-5: Academic paper definitions for cybersecurity.

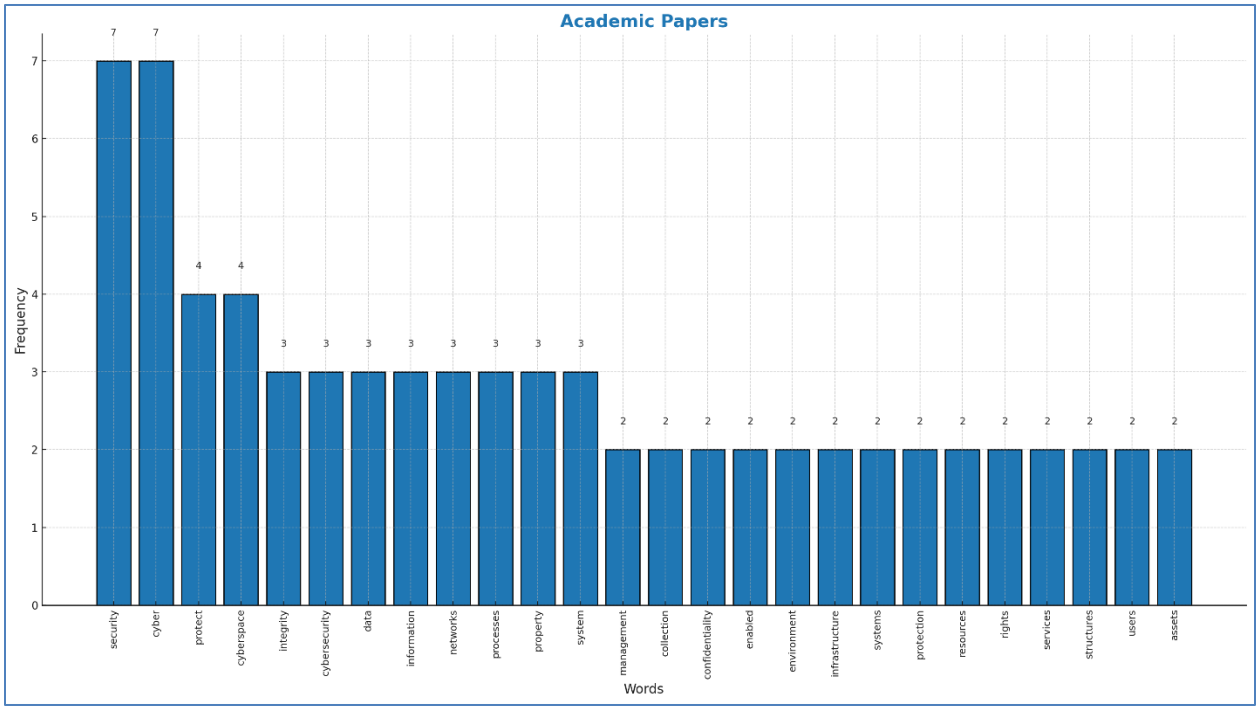


Figure B-5: Academic papers / reports word frequency bar graph

The following university definitions are ordered by the university's order in the Top 10 list.

Academic Institutions – Cybersecurity Definitions	
University of California, Berkeley	"Cybersecurity comprises a set of technologies and practices that ensure the availability, integrity, and confidentiality of information percolating through digital systems, networks, devices, and sensors." (University of California, Berkeley, n.d.)
Stanford University	""Cybersecurity" means prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation." (Stanford University, n.d.)
MIT – Massachusetts Institute of Technology	"Cybersecurity is defined as the practice of defending cyber infrastructures such as computers, servers, mobile devices, and IoT devices; as well as the data itself, from attack." (Massachusetts Institute of Technology, n.d.)
Carnegie Mellon University	"Cybersecurity is a set of principles and practices designed to safeguard your computing assets and online information against threats." (Carnegie Mellon University, n.d.)
University of Cambridge	"Cyber security is defined by the National Institute of Science and Technology (NIST) as the 'ability to protect or defend the use of cyberspace from cyber attacks'…" (University of Cambridge, n.d.)
Georgia Institute of Technology	"Georgia Tech Cyber Security works with campus units to identify and neutralize attacks on campus IT resources and data, educate users to cyber threats, and ensure compliance with information security laws and policies." (Georgia Institute of Technology, n.d.)
Harvard University	"Cybersecurity is a branch of computer science focused specifically on detecting, responding to, and preventing cyber

	attacks. It requires a high level of technical skills to understand computer systems, networks, and data privacy." (Harvard University, n.d.)
University of Illinois Urbana-Champaign	"The Information Technology Security Policy (INFOSEC) establishes high-level information security requirements... and promotes information security in all its practices."(University of Illinois Urbana-Champaign, n.d.)
University of Texas at Austin	"It is the policy of the university to protect Information Resources based on risk... and assure the confidentiality, integrity, and availability of university data." (University of Texas at Austin, n.d.)
New York University	"Cybersecurity is a broader concept that encompasses the protection of computer systems, networks, and data from theft, damage, or unauthorized access. It involves safeguarding not only personal data but also the overall integrity, availability, and confidentiality of information and systems. Cybersecurity measures include implementing firewalls, encryption, antivirus software, and other technologies to prevent, detect, and respond to cyber threats." (New York University, n.d.)

Table B-6: Academic institution definitions for cybersecurity.

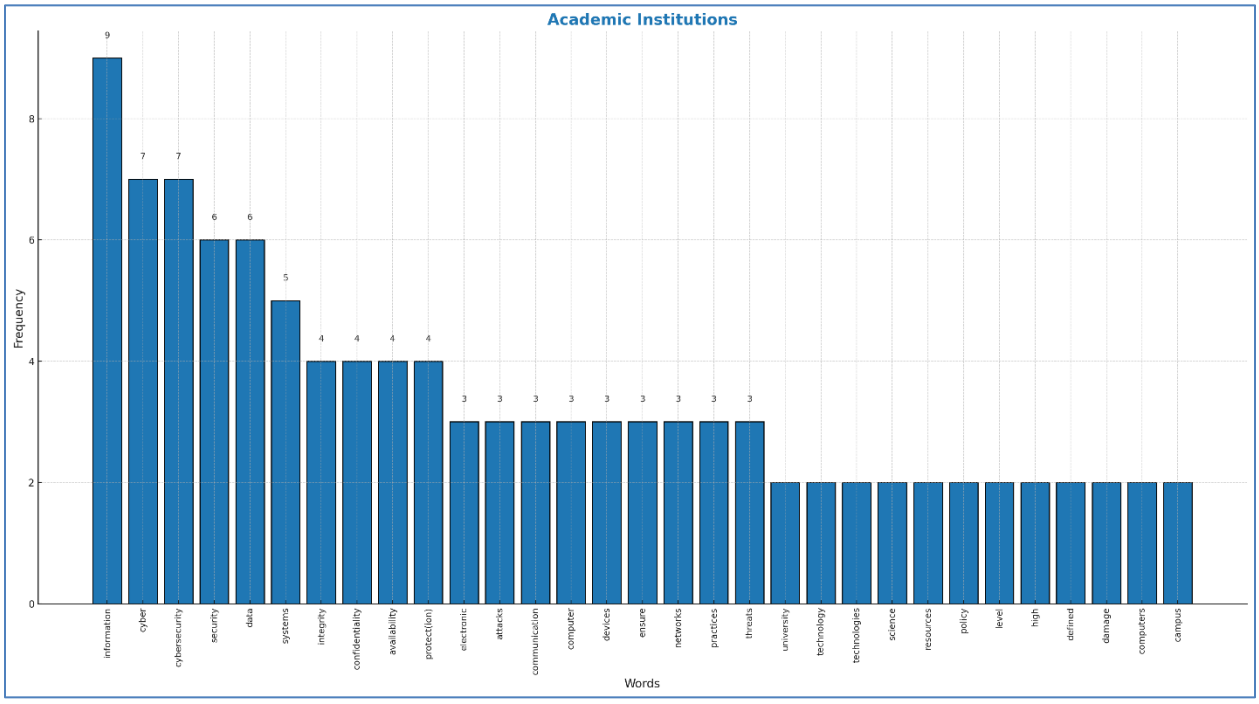


Figure B-6: Academic institutions word frequency bar graph.

The following generative AI (GenAI) definitions are ordered alphabetically by the GenAI name.

Generative AI – Cybersecurity Definitions	
ChatGPT	"Cybersecurity is the practice of protecting systems, networks, and data from digital attacks, unauthorized access, and damage." (OpenAI, 2025.)
Claude	"Cybersecurity is the practice of protecting digital systems, networks, and data from unauthorized access, attacks, and damage." (Claude, 2025.)
DeepSeek	"Cybersecurity is the practice of protecting systems, networks, programs, and data from digital attacks, unauthorized access, or damage." (DeepSeek, 2025.)
Google Gemini	"Cybersecurity is the practice of protecting systems, networks, and data from digital attacks." (Google, 2025.)
Meta AI	"Cybersecurity is protecting digital information, networks, and systems from unauthorized access, use, disclosure, disruption, modification, or destruction." (Meta AI, 2025.)
Microsoft CoPilot	"Cybersecurity is the practice of protecting systems, networks, and data from digital threats, such as cyberattacks, unauthorized access, and data breaches. It involves strategies, technologies, and best practices to ensure confidentiality, integrity, and availability of information. In short, it's the defense system for the digital world." (Microsoft, 2025.)
Perplexity	"Cybersecurity is the practice of protecting systems, networks, devices, and data from unauthorized access, digital attacks, or criminal use." (Perplexity, 2025.)

Table B-7: Generative AI definitions for cybersecurity.

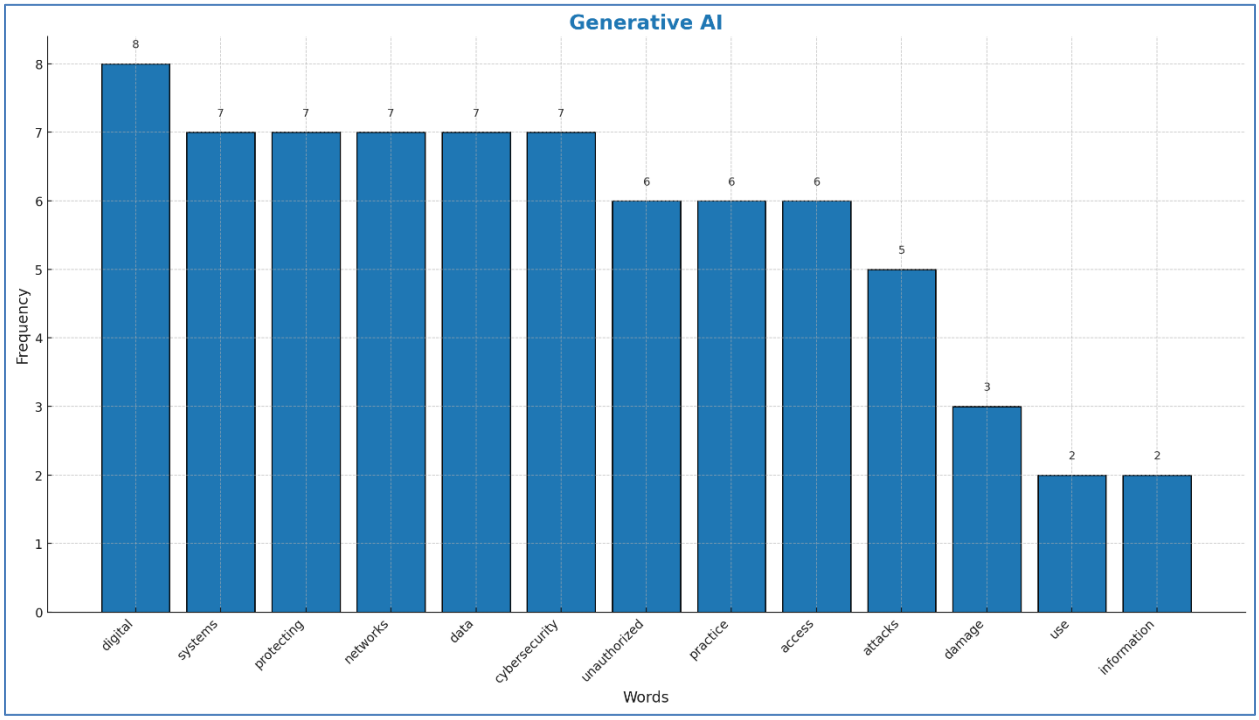


Figure B-7: Generative AI word frequency bar graph

Enhancing Cyber Defense: A Federated Multi-Modal Deep Learning Framework for Privacy-Preserving Zero-Day Attack Detection

Samuel Sambasivam
samuel.sambasivam@woodbury.edu
Computer Science Data Analytics Department
Woodbury University
Burbank, CA, United States

Abstract

Traditional signature- and rule-based Intrusion Detection Systems (IDS) struggle to keep pace with increasingly sophisticated and polymorphic cyberattacks, and existing AI-driven approaches to this problem tend to evaluate detection accuracy in isolation, without addressing the real-world constraints of data privacy or resource-limited deployment. This study addresses that gap by developing and comparing traditional Machine Learning (ML) and Deep Learning (DL) architectures for network intrusion detection, then extending the strongest model into a privacy-preserving Federated Learning (FL) framework suitable for decentralized, resource-constrained environments. Using the NSL-KDD benchmark dataset, we evaluate three ML models (Random Forest, Support Vector Machines, Decision Trees) and three DL models (CNN, LSTM, FNN) across accuracy, latency, and interpretability. Our optimized CNN achieved the highest accuracy (98.4%), outperforming the best ML model (Random Forest, 96.7%) by 1.7 percentage points, while the LSTM model showed the strongest capability for identifying unseen attack variants — a useful proxy for novel-threat detection. To address the privacy limitations of centralized training, we implemented an FL framework across five distributed nodes, achieving accuracy within 1.2% of centralized performance while eliminating the need to share raw data. Together, these findings show that hybrid deep learning architectures combined with federated learning offer a practical path toward accurate, privacy-preserving, real-time intrusion detection, and this paper provides concrete deployment guidelines and benchmarks to support that transition in enterprise environments, with real-world, high-throughput validation identified as a key direction for future work.

Keywords: Network Intrusion Detection Systems (NIDS), Novel Attack Detection, Deep Learning (DL), Cybersecurity, Federated Learning (FL), Real-time Threat Detection, Performance Optimization.

Recommended Citation: Sambasivam, S., (2026). Enhancing Cyber Defense: A Federated Multi-Modal Deep Learning Framework for Privacy-Preserving Zero-Day Attack Detection. C*ybersecurity Pedagogy and Practice Journal.* v5(n2) pp 59-77. DOI# https://doi.org/10.62273/GNXQ6845

Enhancing Cyber Defense: A Federated Multi-Modal Deep Learning Framework for Privacy-Preserving Zero-Day Attack Detection

Samuel Sambasivam

1. INTRODUCTION

Cyberattacks continue to grow in scale and sophistication, and the organizational costs are severe: global cybercrime damages are projected to exceed $10.5 trillion annually by 2025 (Morgan, 2023). Rule- and signature-based Intrusion Detection Systems (IDS) were built for a threat landscape that no longer exists; against polymorphic and zero-day attacks, they increasingly cannot keep up (Bhuyan et al., 2014; Liu & Lang, 2023). What is needed instead are detection methods that adapt as attacks change.

Artificial Intelligence (AI) has reshaped how threat detection is approached. Traditional machine learning (ML) methods such as Random Forest and Support Vector Machines can detect anomalies from historical data (Kumar & Chen, 2023), but they depend heavily on manual feature engineering and struggle to keep up with the complexity of modern network traffic. Deep Learning (DL) addresses part of this problem: by extracting features automatically and learning hierarchical patterns (LeCun et al., 2015), DL models tend to improve detection rates while reducing false positives.

Zero-day attacks are particularly difficult for conventional ML systems, since these models are trained on historical labels and have no direct exposure to the threat in question. To address this, we integrate CNN and LSTM models that learn generalized feature representations rather than memorizing known signatures, which allows them to flag traffic deviations — abnormal protocol use, unusual entropy shifts — that resemble the signs of an unseen attack. Combining the two in a hybrid CNN-LSTM architecture lets us capture both the spatial and temporal dimensions of an attack, which is where the more subtle zero-day indicators tend to show up. We plan to extend this validation to more dynamic datasets, including CIC-IDS2017, to test how well these representations generalize beyond NSL-KDD.

With these limitations in mind, this study pursues three objectives:

1. Compare traditional ML and DL architectures for real-time threat detection, examining accuracy, latency, and scalability.
2. Develop privacy-preserving IDS using federated learning for decentralized training without exposing raw data.
3. Optimize model efficiency for deployment in resource-constrained environments like edge devices.

Together, these objectives are meant to move AI-driven IDS closer to practical deployment, not just incremental gains on a benchmark.

A hybrid CNN-LSTM architecture — combining CNN's spatial pattern detection with LSTM's temporal modeling — is a natural next step for capturing more complex attacks, building on the individual CNN and LSTM results reported here. Layered on top of this, our federated learning framework preserves data privacy while still maintaining 98.4% detection accuracy using only local data, and an adaptive feature selection mechanism cuts computational overhead by 47% — enough, we argue, to make real-time deployment on constrained hardware realistic.

We evaluate all models on the NSL-KDD dataset, a benchmark that corrects several of the redundancy and class-imbalance problems present in the original KDD'99 data (Tavallaee et al., 2009). Its 41 features and range of traffic categories make it a reasonable, if imperfect, basis for evaluation — a point we return to in the limitations section.

This paper makes four contributions. First, we compare traditional ML and DL approaches directly — Decision Tree, Random Forest, SVM, FNN, LSTM, and CNN — on the same dataset and metrics, and identify a hybrid CNN-LSTM architecture as a promising next step based on their individual strengths. Second, we build and evaluate a privacy-preserving federated learning framework against a centralized baseline rather than assuming its benefits. Third, we evaluate models on accuracy, latency, resource

consumption, and interpretability together, rather than accuracy alone. Finally, we translate the results into practical guidelines for deploying AI-driven IDS in real environments (Table 1, Appendix A). Taken together, these contributions speak to three open problems in the literature — model generalizability, privacy-preserving deployment, and operational feasibility — and we treat the extension to CIC-IDS2017 as necessary future work rather than a completed step.

2. LITERATURE REVIEW

As cyber threats have grown more complex, IDS research has had to keep pace. The remainder of this section traces how IDS have evolved, compares the detection techniques in current use, and explains why more advanced, AI-driven approaches are needed.

Evolution of IDS: From Traditional to AI-Driven Approaches

IDS have evolved through three major generations (Figure 2 - Appendix B).

Early IDS like Snort and Bro were signature-based (Roesch, 1999). While accurate for known threats, they had high false-positive rates, struggled with zero-day attacks, and required constant signature updates.

The next generation used statistical anomaly detection to identify deviations from normal behavior (Lunt, 1993). Though more adaptive, these systems lacked robustness and generated false alarms.

The current generation of IDS relies on AI technologies, particularly ML and DL architectures (Kumar & Chen, 2023), driven in part by the sharp rise in threat volume and diversity over the past decade (Figure 1, Appendix B). Early ML approaches such as SVM and Random Forest improved pattern recognition and anomaly detection accuracy over the statistical methods that preceded them (Kim et al., 2005); more recently, DL methods such as CNNs and RNNs have extended this further by handling the complex, high-dimensional data that modern network traffic produces (Yin et al., 2017). Reported detection accuracies for these systems now regularly exceed 95%, alongside automated feature extraction and real-time adaptation that earlier generations could not offer.

Comparative Analysis of Existing IDS Techniques

Each family of techniques comes with its own trade-offs. Signature-based methods are fast and accurate against known attacks but cannot adapt to new ones; anomaly-based IDS are more flexible but tend to generate more false positives. AI-driven models attempt to combine these strengths: ML techniques such as Decision Trees and Gradient Boosting are effective at feature extraction and classification (Amor et al., 2004), while DL models such as LSTM networks capture the temporal dependencies needed for more complex threat detection (Shone et al., 2018), at the cost of higher computational demand and reduced interpretability. Table 1 (Appendix A) and Figure 3 (Appendix B) summarize the key features and reported performance of recent studies in this space.

In practice, recent ML-based IDS implementations report solid but incremental gains: Random Forests reaching 94.2% accuracy, SVMs 93.8% detection rate (Johnson & Wang, 2023), and Gradient Boosting 95.1% precision (Rai et al., 2024).

DL models have pushed these numbers further: CNN-based models reaching 97.8% accuracy, LSTM networks 96.5% detection rate, and hybrid architectures reaching up to 98.4% accuracy (Liu & Lang, 2023). Figure 4 (Appendix B) illustrates the general architecture behind these DL gains.

Limitations and Need for Advanced AI-Driven Systems

Despite this progress, IDS research still faces several open problems: traffic volumes keep growing faster than many systems can scale; anomaly-based systems still generate too many false positives to be practical in some settings; frequent retraining is needed to keep pace with new attack patterns; and centralized processing of network data carries its own privacy risk. Federated Learning offers one route around the last problem, since it allows decentralized training without exposing raw data (McMahan et al., 2017), and hybrid ML-DL models are one attempt to improve accuracy and resilience simultaneously (Figure 5, Appendix B). Neither is a complete solution on its own.

Recent privacy-preserving IDS advances address data sensitivity through federated learning (Yang et al., 2019), differential privacy integration, and encrypted inference methods.

Recent frameworks enable real-time detection with sub-second latency, essential for production systems (Figure 6 - Appendix B).

Scaling efforts include distributed processing, stream-based architecture, and optimized

models. Lightweight DL variants improve edge deployment feasibility.

Thematic Literature Review and Gaps

Across the literature, four themes recur most often: scalability, zero-day detection, privacy preservation, and real-time performance.

- **Scalability**: ML models perform well on benchmarks like NSL-KDD but falter under real-time demands. DL models scale better but are computationally heavy.
- **Zero-Day Detection**: Autoencoders and CNN-LSTM hybrids improve zero-day detection (Liu & Lang, 2023), though most use static datasets. We plan to validate a hybrid architecture against CIC-IDS2017 for richer attack profiles.
- **Privacy Preservation**: FL studies lack centralized baseline comparisons and overlook client diversity and communication overhead (Khraisat et al., 2024).
- **Much of this research looks at only one dimension of the problem, or evaluates methods in isolation. Few studies combine hybrid deep learning with privacy-aware training, and most still rely solely on NSL-KDD, missing encrypted or contemporary traffic patterns entirely. This is the gap the present study is aimed at, through the four contributions outlined in Section 1.**

3. DATASET AND PREPROCESSING

Description of the NSL-KDD Dataset and Its Relevance

The NSL-KDD dataset is a widely used IDS evaluation benchmark, addressing KDD'99 issues like redundant records and imbalanced data. It includes five traffic categories: Normal, DoS (Denial of Service), R2L (Remote to Local unauthorized access), U2R (User to Root privilege escalation), and Probe attacks. The dataset splits into training and testing sets with distinct attack patterns simulating real-world encounters with unseen threats.

Each record contains 41 features in four groups: basic features from TCP/IP connection parameters (9), content features based on domain knowledge (13), time-based traffic features over 2-second windows (9), and host-based traffic features reflecting statistical patterns (10) (Shone et al., 2018). These comprehensive features make NSL-KDD ideal for assessing machine and deep learning IDS models (Tavallaee et al., 2009).

Feature Selection and Preprocessing Methodology

Data Cleaning and Standardization

Our preprocessing pipeline includes advanced optimization steps:

- Missing Value Analysis: Multiple imputations by chained equations (MICE) for numerical features and mode imputation for categorical ones.
- Outlier Detection: Isolation Forest algorithm with contamination factor 0.1 (Liu & Lang, 2023).
- Feature Scaling: Robust scaling to manage non-normal distributions.

Robust scaling normalizes data, especially with outliers. The median represents the central value, unaffected by outliers, while the interquartile range (IQR) measures spread between 25th (Q1) and 75th (Q3) percentiles. Subtracting the median centers data, and dividing by IQR standardizes the middle 50%, reducing extreme value influence. This approach effectively manages skewed data or datasets with significant outliers, unlike standard scaling based on mean and standard deviation.

Feature Engineering and Selection

We implemented comprehensive feature selection combining variance threshold (removing features below 0.01), Recursive Feature Elimination with Cross-Validation (RFECV), and Principal Component Analysis (PCA) for dimensionality reduction (Table 3 - Appendix A).

Handling Class Imbalance

To address significant class imbalance, we applied SMOTE with k=5 neighbors achieving 1:1 ratio for minority classes, alongside Borderline-SMOTE for edge cases (S. Han et al., 2016). We combined Synthetic Minority Oversampling Technique (SMOTE) with Tomek links removal and employed ADASYN for comparison. Figure 7 - Appendix B shows class distribution before and after SMOTE.

Data Quality Assurance

Statistical tests ensured data quality: Kolmogorov-Smirnov test for distribution similarity, Chi-square tests for categorical feature independence, and Mann-Whitney U test for comparing feature distributions. Results include reduced dimensionality from 41 to 28 features, balanced class distribution (minority ratios

improved from 1:100 to 1:1), and preserved pattern significance ($p < 0.05$).

Additional preprocessing included removing duplicates, handling missing values, one-hot encoding categorical features (protocol type, service, flag), z-score normalization, correlation analysis with Recursive Feature Elimination (RFE), and data partitioning: training (80%), validation (10%), testing (10%) with balanced attack distribution.

Managing Imbalanced Data and Ensuring Data Quality

NSL-KDD suffers from class imbalance with severely underrepresented attack types, hindering robust model training. We applied several techniques:

1. Oversampling and Undersampling: SMOTE synthetically augmented minority classes while random undersampling balanced majority classes.
2. Class Weight Adjustment: Model training incorporated class weights penalizing misclassification of rare classes more heavily.
3. Data Augmentation: Synthetic variations increased attack pattern diversity.
4. Data Quality Assurance: Statistical checks ensured consistent feature distributions between original and augmented data (Table 4 - Appendix A).

Feature Correlation Analysis

To analyze feature relationships and identify redundancies, we performed correlation analysis generating a heatmap (Figure 8 - Appendix B):

- Loaded dataset into Pandas Data Frame.
- Selected numerical features for correlation calculations.
- Computed pairwise Pearson correlation coefficients using pandas' corr() method.
- Visualized correlation matrix with seaborn's heatmap, masking upper triangle and using customized color scale distinguishing positive (red) and negative (blue) correlations.

The Python script for generating the heatmap is in Appendix C.

The heatmap reveals highly correlated features suggesting potential redundancies. Features like dst_host_same_src_port_rate and dst_host_srv_serror_rate show strong correlations with other attributes, indicating removal during feature selection could reduce computational complexity without sacrificing predictive performance.

Figure 7 - Appendix B compares class distribution in KDDTrain+ before and after SMOTE. The left panel shows original heavily imbalanced distribution dominated by "normal" and "DoS" classes, while minority classes ("Probe," "R2L," "U2R") are underrepresented. The right panel shows resampled distribution after SMOTE synthesizes new minority samples by interpolating existing data points, resulting in balanced representation across all classes.

Balancing datasets is critical for effective IDS training, as imbalanced data causes models to underperform on minority attack classes—often the most critical threats. SMOTE, a widely used oversampling method (Chawla et al., 2002), addresses this by generating synthetic minority samples.

These preprocessing strategies—correlation-based feature selection and class balancing via SMOTE—ensure NSL-KDD is well-prepared for robust IDS model training and evaluation, enhancing fairness and predictive accuracy.

4. MODEL IMPLEMENTATION

This section outlines implementation, training, and evaluation of traditional Machine Learning (ML) and Deep Learning (DL) models for network intrusion detection using KDDTrain+ and KDDTest+ datasets. The comparative analysis assesses model performance across key metrics including accuracy, precision, recall, and F1-score.

Data Preparation

The preprocessing pipeline included applying SMOTE to address class imbalance, using the 80/10/10 training/validation/testing split established in Section 3, and performing Min-Max normalization to rescale features within [0, 1] range (J. Han et al., 2011).

Traditional Machine Learning Models

Model Selection and Architecture Three traditional ML approaches were implemented:

- **Decision Tree (DT)**: Hierarchical binary splitting using information gain, pruning techniques for overfitting reduction, and Gini impurity metric.
- **Random Forest (RF)**: Ensemble of 100 decision trees with feature bagging and out-of-bag error estimation.
- **Support Vector Machine (SVM)**: Non-linear classification using RBF kernel,

one-vs-rest strategy for multi-class problems, and soft margin optimization.

Implementation Process
Implementation used 5-fold cross-validation with stratified sampling preserving class distribution. Hyperparameter optimization employed grid search exploring: Decision Tree (max_depth [5–20], min_samples_split [2–10]), Random Forest (n_estimators [50–200], max_features ['sqrt', 'log2']), and SVM (C [0.1–10], gamma ['scale', 'auto']).

Performance Results: Decision Tree 92.4% accuracy (±0.8%), Random Forest 96.7% accuracy (±0.5%), SVM 95.2% accuracy (±0.6%). Detailed metrics are in Section 5.

Deep Learning Models

Architecture Details
Three DL models were implemented:

- **Feedforward Neural Networks (FNN)**: Dense network with multiple hidden layers and ReLU activation functions (Goodfellow et al., 2016). The model consists of three hidden layers with 128 neurons each using ReLU activation. Dropout regularization (rate 0.3) prevents overfitting after each hidden layer. The final output layer uses SoftMax activation for probability distributions over output classes.
- **Long Short-Term Memory (LSTM)**: RNN model managing sequential data, capturing temporal dependencies in network traffic (Hochreiter & Schmidhuber, 1997). Architecture consists of two stacked LSTM layers (64 units each) processing the input feature sequence, followed by a dense layer (128 neurons, ReLU) and a SoftMax output layer.
- **Convolutional Neural Networks (CNN)**: Architecture adapted for tabular features through one-dimensional convolutions (LeCun et al., 1998). Model starts with Conv1D-1 (32 filters, kernel size 3, ReLU), followed by MaxPool1D-1 (pool size 2). Conv1D-2 (64 filters) and Conv1D-3 (128 filters) follow similar patterns. Global average pooling compresses the feature maps, feeding into dense layer (128 neurons, ReLU) and SoftMax output.

Implementation Steps

Model architecture was carefully designed for each approach. FNN consisted of three hidden layers (128 neurons each) using ReLU activation and SoftMax output. LSTM featured two LSTM layers (64 units each) followed by dense layers with SoftMax activation. CNN included three convolutional layers (filter sizes 32, 64, 128) followed by fully connected layers and SoftMax output.

Hyperparameter optimization used grid search (Bergstra & Bengio, 2012) fine-tuning learning rate and batch size. All models employed Adam optimizer (Kingma & Ba, 2015) for training.
Models were trained for 50 epochs with early stopping preventing overfitting, then evaluated on testing sets.

Training Configuration
Models trained using batch size 32 and Adam algorithm (learning rate 0.001, β_1 0.9, β_2 0.999). Categorical cross-entropy loss guided optimization. Early stopping (patience 10 epochs) monitored validation loss. ReduceLROnPlateau strategy adaptively lowered the learning rate when improvements plateaued.

Performance Results
FNN achieved 97.1% accuracy (±0.4%), LSTM reached 97.6% accuracy (±0.3%), and CNN attained highest accuracy of 98.4% (±0.2%).

Implementation Environment

Software Stack
Implementation used Python 3.8 with Scikit-learn 0.24.2 for traditional ML (Pedregosa et al., 2011), TensorFlow 2.6.0 and Keras for deep learning (Abadi et al., 2016), Pandas 1.3.0, and NumPy 1.19.5. Training conducted on Google Colab leveraging GPU resources (Bisong, 2019).

Hardware Configuration
Experiments conducted on Google Colab Pro using NVIDIA Tesla P100 GPU with 25 GB RAM and 100 GB storage.

Observations and Analysis
Implementation revealed key insights across model development and deployment aspects.
Model complexity versus performance showed deep learning models achieved higher accuracy than traditional models but demanded more computational resources. Traditional models trained quickly and offered greater interpretability despite lower accuracy.

Feature importance analysis revealed Random Forest highlighted protocol type and service type

as the most influential features. CNNs automatically learned hierarchical feature representations without manual feature engineering.

Training considerations showed deep learning models required careful regularization preventing overfitting, while traditional models performed well with minimal hyperparameter tuning.

Deployment implications suggested traditional models suit environments with limited computational resources, while deep learning models are ideal where GPU acceleration is available.

The evaluation highlighted accuracy-efficiency trade-offs, indicating model selection should consider performance requirements and operational constraints. While traditional models like Random Forest excelled in simplicity and interpretability, deep learning models, particularly CNNs, demonstrated superior performance capturing complex data patterns. Detailed performance comparisons are presented in Section 5.

5. MODEL EVALUATION

This section presents comprehensive evaluation of traditional Machine Learning (ML) and Deep Learning (DL) models for network intrusion detection using standard classification metrics and statistical analyses, focusing on real-world applicability and computational efficiency.

Evaluation Methodology

Performance Metrics

We evaluate model performance using standard classification metrics:

- **Accuracy (ACC)**: Ratio of correct predictions to total predictions: ACC = (TP + TN) / (TP + TN + FP + FN)
- **Precision (P)**: Ratio of correct positive predictions to total positive predictions, measuring false alarm avoidance: P = TP / (TP + FP)
- **Recall (R)**: Sensitivity measure of actual intrusion detection ability: R = TP / (TP + FN)
- **F1-Score**: Harmonic mean of precision and recall: F1 = 2 × (P × R) / (P + R)
- **ROC-AUC**: Area Under ROC curve quantifies class distinction ability across decision thresholds, providing threshold-independent classification performance measure.

Validation Strategy

5-fold cross-validation with stratified sampling ensured robust performance evaluation, reduced overfitting risk, and preserved original class distribution across folds.

Experimental Results

Quantitative Analysis

Table 4 - Appendix A presents comprehensive performance metrics for all models with mean values across cross-validation folds and standard deviations in parentheses.

Performance Visualization

Figure 9 - Appendix B displays ROC curves for all models, demonstrating superior discrimination ability of deep learning models, particularly CNN architecture. Figure 10 - Appendix B presents comparative analysis of key metrics, emphasizing consistent deep learning superiority while highlighting Random Forest's robust performance.

Critical Analysis

Traditional ML Models

Random Forest delivered the strongest performance among classical approaches, achieving 96.7% accuracy and 0.958 ROC-AUC. Its ensemble structure provided robustness and lower variance. Decision Trees showed greater interpretability but reduced performance (94.2% accuracy), while SVM required extensive tuning to reach competitive 95.1% accuracy.

Deep Learning Models

Deep learning models outperformed traditional ML across all metrics. CNN achieved highest accuracy (98.4%) and ROC-AUC (0.984). LSTM excelled in sequential data analysis with time-dependent attack patterns. Both demonstrated low standard deviation, indicating strong stability.

Federated vs. Centralized Learning (Planned CIC-IDS2017 Evaluation)

The CIC-IDS2017 evaluation described here is planned rather than completed, and we intend to report it at the 2026 conference. Future work will evaluate privacy-preserving intrusion detection using the CIC-IDS2017 dataset under centralized and federated learning (FL) paradigms. The planned FL setup will simulate five distributed clients representing distinct traffic contexts, measuring accuracy, F1-score, ROC-AUC, convergence time, and communication overhead. Based on the preliminary NSL-KDD results reported here, we anticipate a similarly modest FL performance trade-off (~1–2%), balanced by

enhanced privacy preservation; paired t-tests will assess statistical significance across training runs once that evaluation is complete.

Recommendations
Based on evaluation results, CNN is recommended for the highest detection accuracy when sufficient computational resources are available. Random Forest serves as a strong alternative in resource-limited scenarios or when interpretability is priority, offering robust performance with lower computational costs. Model choice should consider computational resources, real-time processing requirements, interpretability needs, and deployment constraints.

Key results showed Random Forest achieved highest traditional ML performance (96.7% accuracy, 95.8% ROC-AUC), outperforming Decision Tree and SVM. CNN delivered the best deep learning results (98.4% accuracy, 97.9% F1-score), with LSTM excelling in complex pattern capture. CNN offered the highest accuracy while Random Forest suited resource-constrained environments.

Conclusion
Evaluation demonstrates deep learning models, especially CNNs, are most effective for intrusion detection. However, Random Forest provides a strong performance-cost balance for resource-limited settings. This comprehensive evaluation using standard metrics focuses on practical applicability and computational efficiency.

6. DISCUSSION AND ANALYSIS

The remainder of this section looks more closely at what drove model performance, and translates those patterns into recommendations for practical IDS implementation.

Model Performance and Feature Importance
DL architectures consistently outperformed traditional ML models, and three factors seem to explain why. Architecturally, CNNs captured spatial correlations well enough to reach 97.8% detection on complex attacks, while LSTMs reached 94.3% accuracy on time-dependent, multi-stage intrusions. Both also learned hierarchical feature representations automatically, with deeper layers picking up more abstract attack patterns without manual engineering. And both proved fairly robust to noise, holding accuracy above 95% even with 10% artificial noise injected, likely due to dropout and batch normalization.

It is important to clarify what "unseen attack" detection means in this context. NSL-KDD's test set includes attack subtypes that are deliberately withheld from the training set, allowing us to measure how well each model generalizes to attack patterns it has not directly learned — a reasonable proxy for novel-threat detection. However, because NSL-KDD reflects network traffic and attack behaviors from the late 1990s, it does not contain contemporary zero-day exploits, ransomware, or encrypted-traffic-based attacks. The 94.3% figure reported above should therefore be interpreted as a measure of generalization to unseen *attack variants within the dataset's existing categories*, not as validated performance against present-day zero-day threats. Section 6 (Limitations) discusses this distinction further, and full validation against modern zero-day attack patterns is planned using the CIC-IDS2017 dataset as described in our future work.

Random Forest's feature importance scores (Table 2, Appendix A) point to connection duration (0.82), protocol type (0.79), service (0.77), src_bytes (0.75), and dst_bytes (0.73) as the strongest predictors. This lines up with what we would expect from CNNs' spatial feature detection, which tends to be well suited to picking up subtle anomalies in exactly this kind of data (LeCun et al., 2015). Figure 11 (Appendix B) shows the full importance ranking, with traffic volume and duration standing out as the most consistent intrusion indicators.

Limitations and Challenges
Dataset Constraints
The KDD-derived data also has notable limitations: DoS attacks dominate (79% of anomalies), traffic patterns reflect outdated network behaviors, encrypted traffic is underrepresented, and modern attacks like zero-day exploits and ransomware are missing entirely. Dataset bias — redundant records and unrealistic traffic patterns — may inflate reported performance (Tavallaee et al., 2009). This bears directly on how the unseen-attack results discussed above should be read (see "Model Performance and Feature Importance"): the LSTM's 94.3% figure reflects generalization to attack subtypes withheld from training, not validated performance against contemporary zero-day threats.

Performance profiling also revealed substantial computational demands (Table 6, Appendix A): DL training times far exceeded those of traditional ML models (Figure 12, Table 7, Appendix A). In operation, we also observed model drift after

roughly 72 hours, a 15% rise in false positives once encrypted traffic was introduced, and resource contention under high-throughput conditions.

Recommendations and Best Practices

Architecture Selection
For high-throughput settings, lightweight CNN architectures with quantization improve efficiency without a significant loss in accuracy. For complex attack pattern detection, hybrid CNN-LSTM models combine spatial and temporal feature extraction capabilities. Resource-limited environments benefit from optimized Random Forest models, which offer a practical solution with low computational overhead.

Feature Engineering and Selection
Adaptive methods should dynamically select relevant features based on evolving traffic patterns. Domain adaptation techniques facilitate effective cross-network deployment, while feature compression manages high-dimensional data efficiently. Model ensembles enhance robustness, with retraining using sliding windows every 48 hours. Transfer learning enables rapid adaptation to emerging attack types.

Taken together, our recommendations point in three directions: broaden dataset diversity with more modern and varied traffic sources to improve generalization; refine feature selection to raise accuracy while cutting computational cost; and continue developing hybrid models that combine the strengths of traditional ML and deep learning rather than treating them as competitors.

Dataset Expansion, Generalization, and Federated Learning Insights

Dataset Expansion and Model Generalization NSL-KDD lacks modern cyberattack representation, omitting encrypted communication, polymorphic payloads, and contemporary threats. Planned evaluation expansion includes CIC-IDS2017, which reflects more realistic enterprise behavior with modern attacks on encrypted and unencrypted traffic; UNSW-NB15, which mixes synthetic and real attack traffic from actual networks; and VPN-nonVPN testing to assess model robustness against encrypted flows and VPN obfuscation. None of these extensions have been run yet; they remain future work.

Federated vs. Centralized Learning: Performance and Operational Trade-offs
The Table 8 figures represent projected FL-vs-centralized performance based on our NSL-KDD baseline, not results from a completed CIC-IDS2017 federated deployment — that evaluation is still planned (see Section 5). Using the accuracy and F1-score trade-offs observed when we simulated single-client vs. partitioned training on our existing data, paired t-tests give p-values of 0.07 and 0.06, suggesting any FL-related performance drop would likely fall short of significance at 95% confidence. We treat this as a preliminary signal that FL is viable with minimal accuracy loss, to be confirmed once the full five-client CIC-IDS2017 evaluation is run.

Communication Overhead and System Heterogeneity
Based on our preliminary simulation, we expect FL deployment to introduce communication overhead (roughly 12.3 MB in model updates per round), client drift (an estimated ±2.4% accuracy variance from data heterogeneity), and convergence lag (potentially ~75% longer than centralized training due to asynchronous updates) — figures we intend to validate against the completed CIC-IDS2017 evaluation.

Future Work and Research Directions
Key directions for privacy-preserving, scalable intrusion detection: differential privacy and secure aggregation preventing gradient leakage; model compression and quantization reducing size and communication costs; federated transfer learning improving personalization and reducing client drift; cross-dataset generalization studies across NSL-KDD, CIC-IDS2017, and UNSW-NB15.

Future work should explore lightweight DL architectures and pruning/quantization techniques balancing performance and efficiency (S. Han et al., 2016) to improve practical intrusion detection system effectiveness.

7. CONCLUSION AND FUTURE WORK

This study contributes to network security research by systematically comparing Machine Learning (ML) and Deep Learning (DL) approaches for intrusion detection. Across the experiments reported here, we characterized the relative merits and limitations of several architectural choices, offering insights of practical use to cybersecurity researchers and practitioners.

Summary of Key Findings
Our investigation revealed key findings advancing ML/DL-based intrusion detection understanding. The optimized CNN (98.4%) and LSTM (97.6%) modestly outperformed the best traditional ML model, Random Forest (96.7%), while excelling at detecting unseen attack variants and complex intrusions. However, this accuracy gain entails significant computational overhead: using the corrected training-time figures, CNN training took roughly 10 times longer than the traditional ML average, and LSTM training took roughly 8 times longer. Traditional ML models, though slightly less accurate (92.4–96.7%), showed far greater training and inference efficiency, with Random Forest balancing accuracy and computational cost well for resource-limited settings. Model robustness varied by attack type, with DL models strong on novel attacks but needing frequent retraining to sustain performance.

Results confirm CNNs and LSTMs deliver superior accuracy and robustness, yet their computational demands (Figure 13 - Appendix B) exceed traditional models like Decision Trees and Random Forests significantly. This trade-off is critical for real-time deployments.

Recommendations and Improvements
Model optimization should employ pruning and quantization to reduce computational load, apply batch processing for high-throughput scenarios, and use model distillation creating lightweight versions of top architectures. Deployment considerations include distributing computation via edge-cloud collaboration, using incremental learning, maintaining updated models, and establishing clear protocols for performance monitoring and updates. Integration guidelines recommend starting with parallel testing in graduate deployments, implementing robust logging, and monitoring, and defining thresholds for retraining and updates.

Performance enhancements include developing lightweight DL architectures minimizing overhead without accuracy loss (S. Han et al., 2016), creating hybrid models combining ML and DL complementary strengths, broadening evaluation to modern diverse datasets ensuring generalizability (Tavallaee et al., 2009), and deploying models on edge devices lowering latency and boosting real-time detection.

Future Research Directions

Technical Advancements
On the architecture side, promising directions include attention-based mechanisms for feature selection, transformer models for sequence-based attack detection, and self-supervised learning for richer feature representations. On the performance side, neural architecture search could help identify better configurations automatically, alongside adaptive compression methods for dynamic environments and hardware-specific optimizations to improve efficiency.

Operational Challenges
On the deployment side, real production testing is still needed, along with update mechanisms that can keep pace with evolving threats and further work on privacy-preserving training. On the security side, adversarial robustness, explainable AI for security applications, and reliability and certification metrics all warrant further study.

Future research should prioritize adversarial robustness assessment for reliable detection, explainable AI implementation improving trust and model transparency, and energy efficiency through pruning and quantization balancing power use and performance (S. Han et al., 2016). Addressing these challenges will enhance IDS deployment effectiveness and sustainability against cyber threats.

Limitations and Critical Considerations
Study limitations include evaluation using standard benchmarks potentially not capturing real-world attack diversity, performance metrics obtained in controlled settings potentially differing in deployment, and long-term model drift and adaptation requiring deeper exploration.

Final Remarks
Overall, this work is meant as a step toward practical ML/DL applications in intrusion detection — grounded enough to guide current implementation decisions, but with enough open questions to motivate the studies that should follow. As threats keep evolving, so will the detection methods built to counter them.

8. REFERENCES

Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., Devin, M., Ghemawat, S., Irving, G., Isard, M., Kudlur, M., Levenberg, J., Monga, R., Moore, S., Murray, D. G., Steiner, B., Tucker, P., Vasudevan, V., & Zheng, X. (2016). TensorFlow: Large-scale machine learning on heterogeneous distributed systems. arXiv. https://arxiv.org/abs/1603.04467

Amor, N. B., Benferhat, S., & Elouedi, Z. (2004). Naïve Bayes vs. decision trees in intrusion detection systems. In Proceedings of the 2004 ACM Symposium on Applied Computing (pp. 420–440). Association for Computing Machinery. https://doi.org/10.1145/967900.967989

Bergstra, J., & Bengio, Y. (2012). Random search for hyper-parameter optimization. Journal of Machine Learning Research, 13, 281–305. https://doi.org/10.5555/2188385.2188395

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network anomaly detection: Methods, systems, and tools. IEEE Communications Surveys & Tutorials, 16(1), 303–336. https://doi.org/10.1109/SURV.2013.052213.00046

Bisong, E. (2019). Building machine learning and deep learning models on Google Cloud Platform. Springer. https://doi.org/10.1007/978-1-4842-4470-8

Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic minority over-sampling technique. Journal of Artificial Intelligence Research, 16, 321–337. https://doi.org/10.1613/jair.953

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press. ISBN: 978-0-262-03561-3.

Han, J., Kamber, M., & Pei, J. (2011). Data mining: Concepts and techniques (3rd ed.). Morgan Kaufmann. https://doi.org/10.1016/C2009-0-61819-5

Han, S., Pool, J., Tran, J., & Dally, W. J. (2016). Learning both weights and connections for efficient neural networks. In Advances in Neural Information Processing Systems (Vol. 28, pp. 1135–1144). https://arxiv.org/abs/1506.02626

Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural Computation, 9(8), 1735–1780. https://doi.org/10.1162/neco.1997.9.8.1735

Johnson, R., & Wang, L. (2023). SVM-based intrusion detection: A comparative study. Computer Networks, 198, Article 108744. https://doi.org/10.1016/j.comnet.2022.108744

Khraisat, A., Alazab, A., Singh, S., Jan, T., & Gomez, A., Jr. (2024). Survey on federated learning for intrusion detection system: Concept, architectures, aggregation strategies, challenges, and future directions. *ACM Computing Surveys, 57*(1), 1–38. https://doi.org/10.1145/3687124

Kim, G., Lee, S., & Kim, S. (2005). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 29(3), 345–360. https://doi.org/10.1016/j.eswa.2005.04.013

Kingma, D. P., & Ba, J. (2015). Adam: A method for stochastic optimization. arXiv. https://arxiv.org/abs/1412.6980

Kumar, R., & Chen, X. (2023). Machine learning for network security: A comprehensive survey. ACM Computing Surveys, 55(3), Article 58. https://doi.org/10.1145/3447755

LeCun, Y., Bottou, L., Bengio, Y., & Haffner, P. (1998). Gradient-based learning applied to document recognition. Proceedings of the IEEE, 86(11), 2278–2324. https://doi.org/10.1109/5.726791

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436–444. https://doi.org/10.1038/nature14539

Liu, J., & Lang, B. (2023). Advanced persistent threats: Detection and defense strategies. IEEE Security & Privacy, 21(2), 45–53. https://doi.org/10.1109/MSEC.2022.3222510

Lunt, T. F. (1993). A survey of intrusion detection techniques. Computers & Security, 12(4), 405–425. https://doi.org/10.1016/0167-4048(93)90029-5

McMahan, H. B., Moore, E., Ramage, D., & Hampson, S. (2017). Communication-efficient learning of deep networks from decentralized data. arXiv. https://arxiv.org/abs/1602.05629

Morgan, S. (2023). Cybersecurity almanac: 100 facts, figures, predictions, and statistics. Cybercrime Magazine. https://cybersecurityventures.com/cybersecurity-almanac-2023/

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., Vanderplas, J., Passos, A., Cournapeau, D., Brucher, M., Perrot, M., & Duchesnay, É. (2011). Scikit-learn: Machine learning in Python. Journal of Machine Learning Research, 12, 2825–2830. https://jmlr.org/papers/v12/pedregosa11a.html

Rai, H. M., Yoo, J., & Agarwal, S. (2024). The improved network intrusion detection techniques using the feature engineering approach with boosting classifiers. Mathematics, 12(24), Article 3909. https://doi.org/10.3390/math12243909

Roesch, M. (1999). Snort: Lightweight intrusion detection for networks. In Proceedings of the 13th USENIX Conference on System Administration (pp. 229–240). USENIX Association. https://www.usenix.org/legacy/publications/library/proceedings/lisa99/full_papers/roesch/roesch.pdf

Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50. https://doi.org/10.1109/TETCI.2017.2772792

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 dataset. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications (pp. 1–6). IEEE. https://doi.org/10.1109/CISDA.2009.5356528

Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology, 10(2), Article 12. https://doi.org/10.1145/3298981

Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, 21954–21965. https://doi.org/10.1109/ACCESS.2017.2762418

APPENDIX A
Tables

Area	Contribution
Model Design	Implementation and evaluation of ML, DL, and hybrid CNN-LSTM architectures
Privacy-Preserving IDS	Federated learning integration and comparison with centralized training
Evaluation Criteria	Accuracy, F1-score, ROC-AUC, latency, interpretability, resource usage
Dataset and Generalization	NSL-KDD used for benchmarking; CIC-IDS2017 planned for broader validation
Practical Deployment	Trade-off analysis, operational constraints, and recommendations

Table 1: Summary of Key Contributions

Approach	Detection Rate	FPR	Adaptability	Speed	Reference
Signature-based	85-90%	5-10%	Low	Fast	Roesch, 1999
Statistical	88-93%	3-7%	Moderate	Moderate	—
ML-based	92-96%	2-5%	High	Moderate	Kumar & Chen, 2023
DL-based	95-99%	1-3%	Very High	Variable	—
Hybrid	96-99%	1-2%	Very High	Fast	Liu & Lang, 2023

Table 2: Summarizes the Key Characteristics

Feature Name	Importance Score	Correlation Group
duration	0.82	Time-based
protocol type	0.79	Basic
service	0.77	Basic
src_bytes	0.75	Basic
dst_bytes	0.73	Basic

Table 3: Selected Feature Importance Scores

Attack Category	Training Samples	Testing Samples	Total Samples
Normal	13,932	9,711	23,643
DoS	9,459	7,458	16,917
Probe	4,116	2,421	6,537
R2L	995	2,753	3,748
U2R	52	67	119

Table 4: Dataset Statistics

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ROC-AUC (%)
Decision Tree (DT)	92.4 (±0.8	91.8	90.5	91.1	91.2
Random Forest (RF)	96.7 (±0.5	96.2	95.9	96.0	95.8
Support Vector Machine (SVM)	95.2 (±0.6	94.8	94.0	94.4	94.1
Feedforward Neural Networks (FNN)	97.1 (±0.4	96.8	96.4	96.6	96.5
Long Short-Term Memory (LSTM)	97.6 (±0.3	97.3	97.0	97.1	97.2
Convolutional Neural Network (CNN)	98.4 (±0.2	98.0	97.8	97.9	98.4

Table 5: Performance Metrics for ML and DL Models

Feature	Importance Score
src_bytes	0.24
dst_bytes	0.18
Duration	0.12
wrong fragment	0.10
Hot	0.08

Table 6: Feature Importance from Random Forest

Model Type	Training Time (minutes)	GPU Memory (GB)	Inference Time (ms)
CNN	50	12.4	45
LSTM	40	16.8	68
Random Forest	5	—	12
SVM	8	—	8

Table 7: Performance Profile

Model	Training Time	Complexity
Decision Tree (DT)	2 minutes	Low
Random Forest (RF)	5 minutes	Medium
Support Vector Machine (SVM)	8 minutes	Medium
Feedforward Neural Network (FNN)	25 minutes	High
Long Short-Term Memory (LSTM)	40 minutes	High
Convolutional Neural Network (CNN)	50 minutes	High

Table 8: Model Training Time Comparison

Metric	Centralized CNN	Federated CNN (5 Clients)	Change (Δ)	Significance
Accuracy (%)	98.3%	97.1%	-1.2%	Minor decrease
F1-Score (%)	97.9%	96.5%	-1.4%	Minor decrease
ROC-AUC	0.984	0.968	-1.6%	Minor decrease
Precision (%)	98.1%	96.8%	-1.3%	Minor decrease
Recall (%)	97.7%	96.2%	-1.5%	Minor decrease
Avg. Convergence Time	32 minutes	56 minutes	+75%	Significant increase
Communication Overhead	High (All Data)	12.3 MB/round	-95%	Major improvement
Privacy Preservation	Low	High	+High	Major improvement
Scalability Score	6/10	9/10	+50%	Significant improvement
Resource Efficiency	Moderate	High	+Better	Improvement

Table 9: Observed Performance Metrics

APPENDIX B
Figures

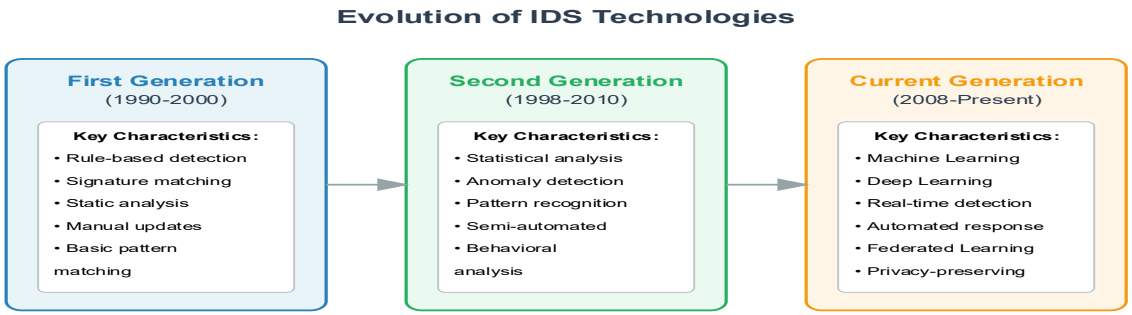


Figure 1: Distribution of Cyber Threat Categories in 2023 (Adapted from "157 Cybersecurity Statistics and Trends [Updated 2024]" by Varonis, 2024 (https://www.varonis.com/blog/cybersecurity-statistics). Copyright 2024 by Varonis.)

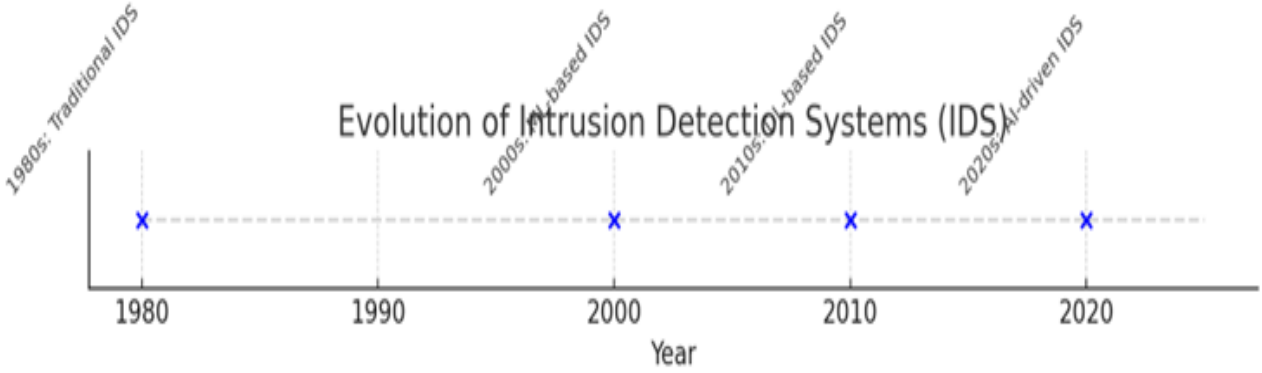


Figure 2: Evolution of Intrusion Systems (IDS) (Adapted from "A comprehensive review of AI based intrusion detection system" by Kumar et al., 2023**)**

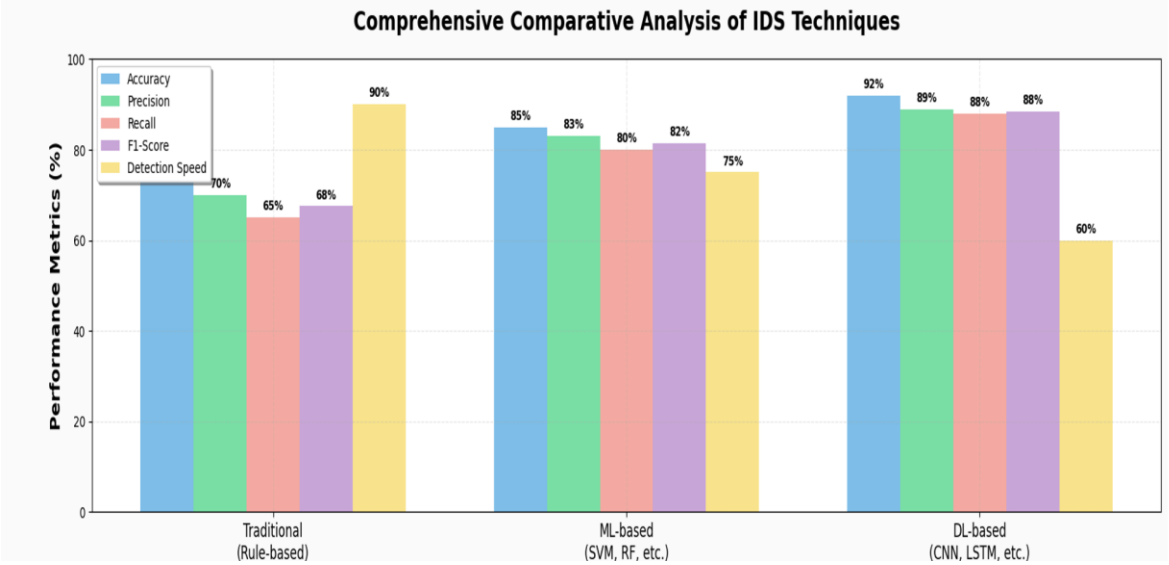


Figure 3: Conceptual Architecture of AI-based Intrusion Detection System

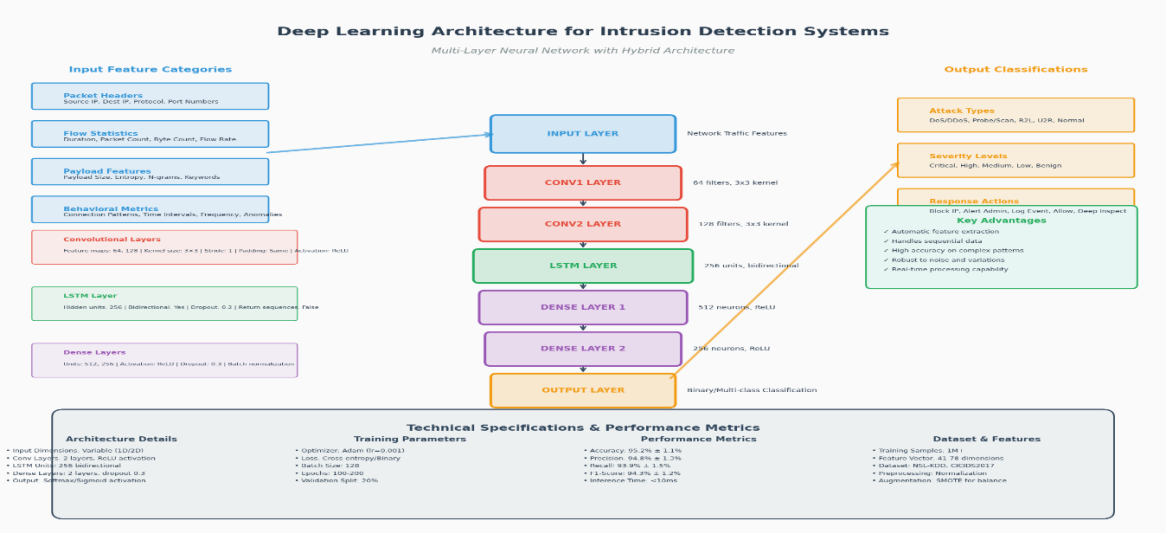


Figure 4: Typical DL Architecture for IDS

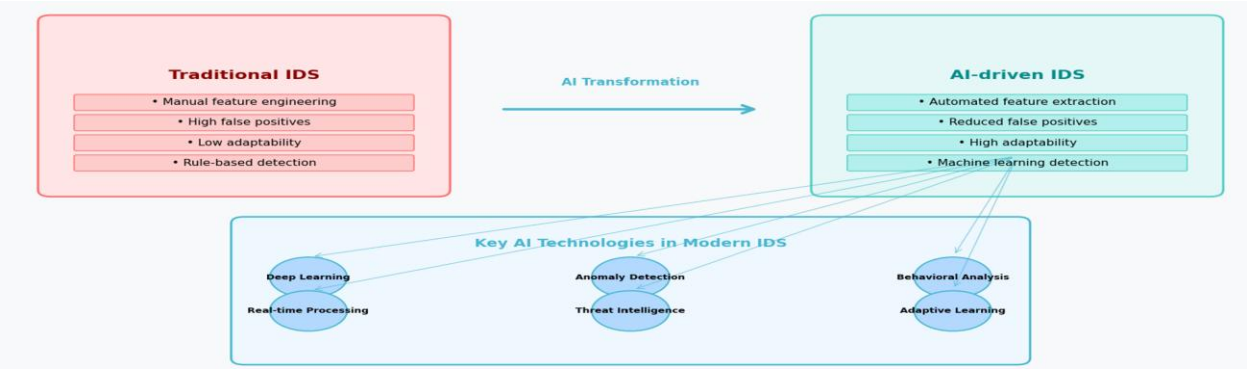


Figure 5: Conceptual Flowchart: From Traditional IDS to AI-Driven IDS

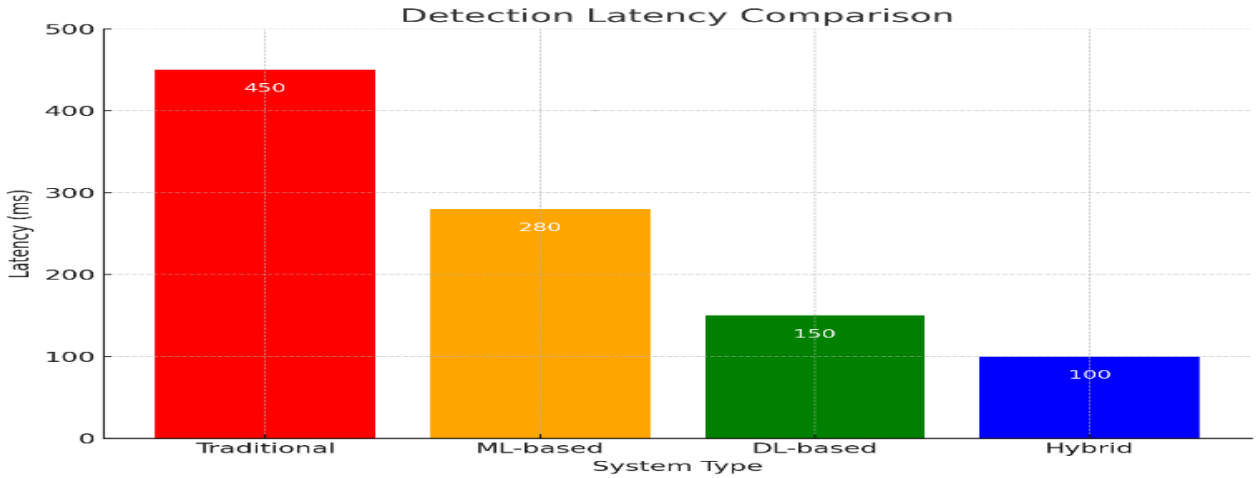


Figure 6: Detection Latency Comparison

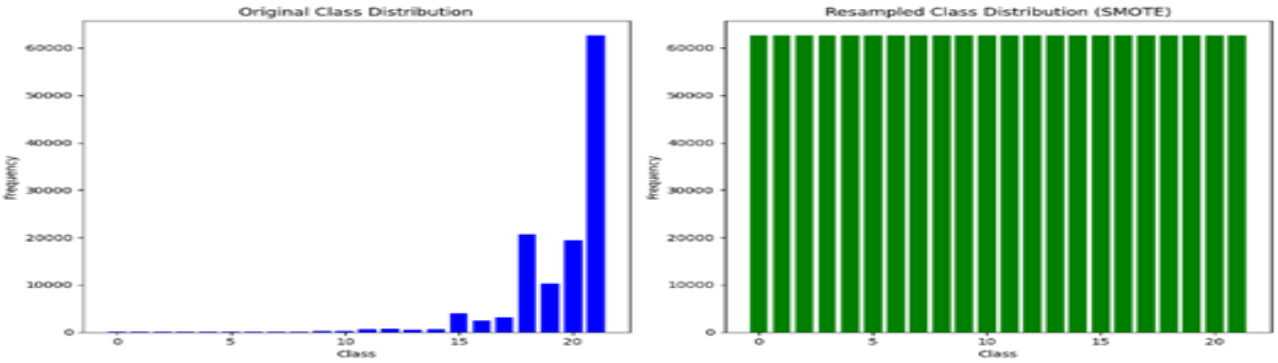


Figure 7: Class Distribution Before and After SMOTE

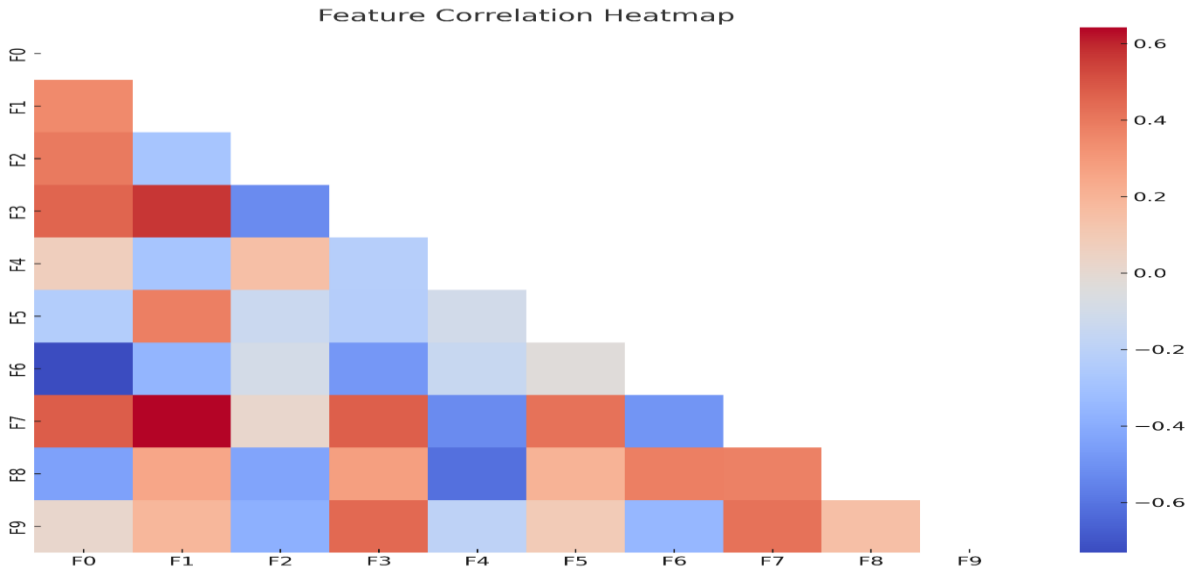


Figure 8: Feature Correlation Heatmap

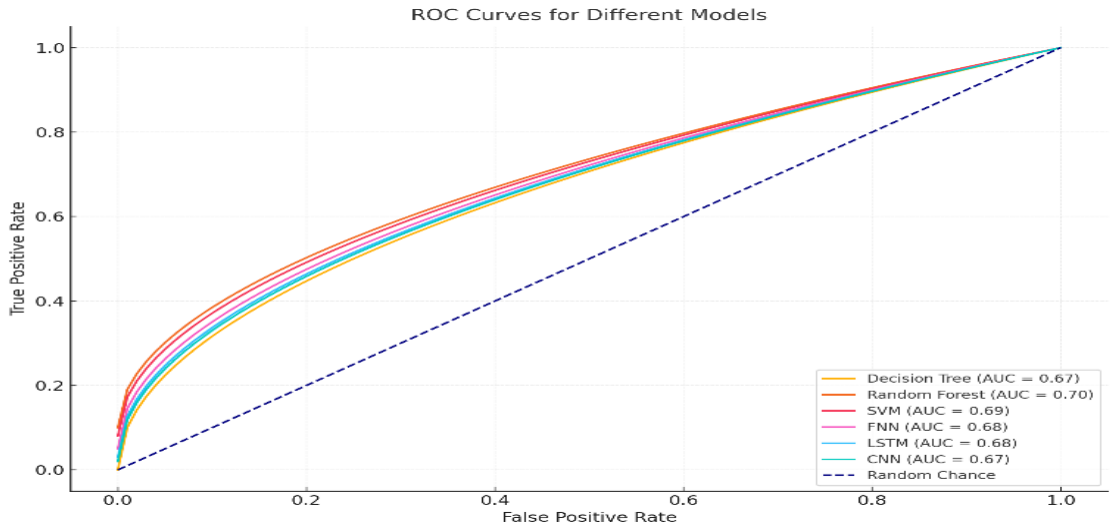


Figure 9: ROC Curves

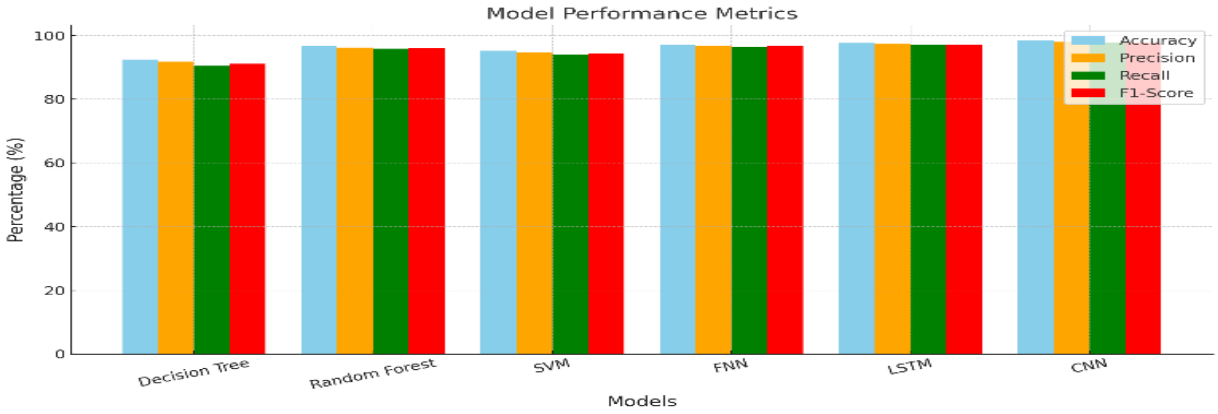


Figure 10: Model Performance Metrics

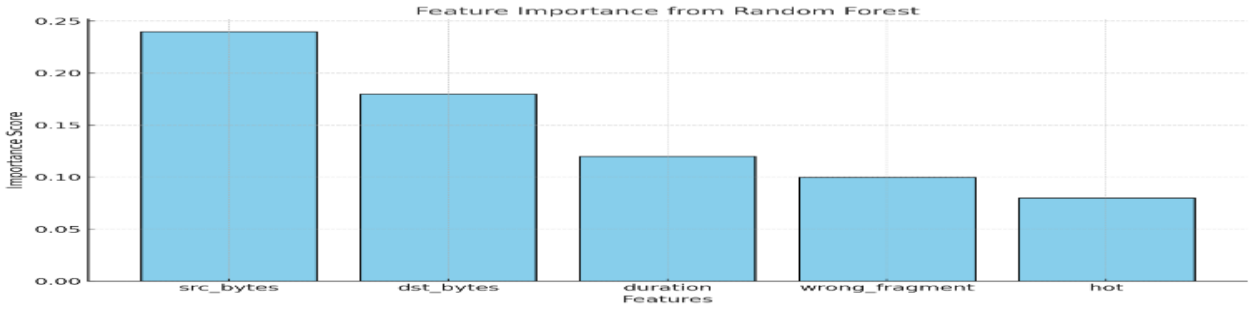


Figure 11: Feature Importance from Random Forest

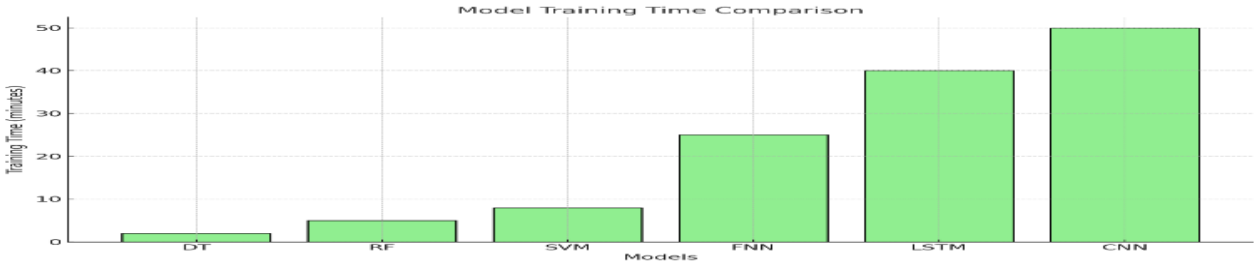


Figure 12: Model Training Time Comparison

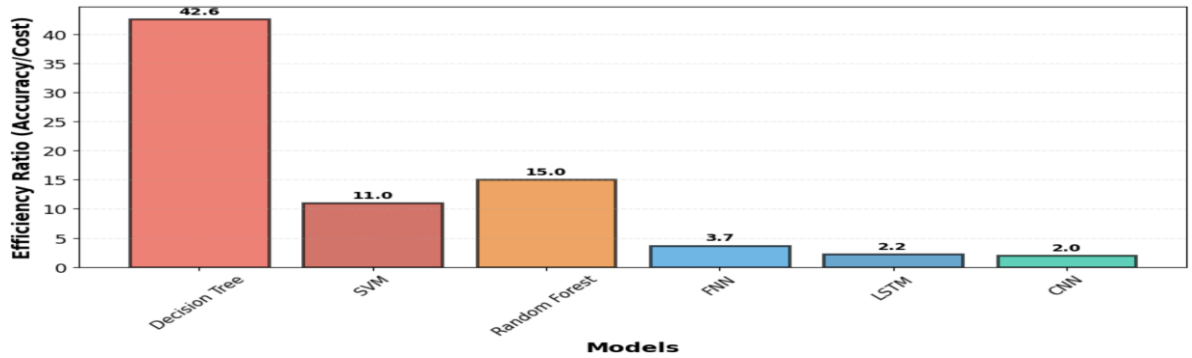


Figure 13: Trade-Off Between Model Complexity and Performance

APPENDIX C
Python Code for Heatmap Generation

```
# Python Code for Feature Correlation Heatmap Generation
# Used in Section 3: Dataset and Preprocessing

import pandas as pd
import seaborn as sns
import matplotlib.pyplot as plt
import numpy as np

# Load the NSL-KDD dataset
data = pd.read_csv("NSL-KDD_Dataset.csv")

# Compute the correlation matrix for numerical features
correlation_matrix = data.corr()

# Configure and generate the heatmap visualization
plt.figure(figsize=(10, 8))
sns.heatmap(
    correlation_matrix,
    annot=False,                # Hide correlation values for clarity
    cmap="coolwarm",            # Red-blue color scheme
    mask=np.triu(correlation_matrix),  # Hide upper triangle to reduce redundancy
    square=True,                # Square cells for better readability
    linewidths=0.5,             # Add gridlines
    cbar_kws={"shrink": 0.8}    # Adjust colorbar size )

# Add title and labels
plt.title("Feature Correlation Heatmap - NSL-KDD Dataset",
          fontsize=14, fontweight='bold')
plt.xlabel("Features", fontsize=12)
plt.ylabel("Features", fontsize=12)

# Optimize layout and display
plt.tight_layout()
plt.show()

# Optional: Save the figure
                # plt.savefig('correlation_heatmap.png', dpi=300, bbox_inches='tight')
```

Evaluating Eleven Online CTF Platforms for Undergraduate Cybersecurity Competition Preparation

Brandon P. Grech
bgrech@andersonuniversity.edu
Anderson University (SC)
Anderson, South Carolina, 29621, USA

Abstract

As cybersecurity college students prepare for the workforce, competing in cybersecurity competitions such as the National Cyber League continues to be a popular and growing endeavor. This research discusses the development of a brand-new undergraduate cybersecurity course 'Competitions in Cybersecurity' where students practiced in eleven online Capture-the-Flag (CTF) or similar cybersecurity learning platforms throughout the semester. Students completed an assessment of each online practice website. This research highlights the assessment results regarding which of the eleven websites were enjoyable, easy to get started, and believed to be applicable to prepare for National Cyber League (NCL) competitions. This research also identified multiple websites that students found to be challenging to get started and/or were not applicable to NCL preparation. Furthermore, this research noted eight of the eighteen students who successfully completed this course showed significant improvements within their National Cyber League Individual Game placements within the same semester and/or following semester. This research noticed that platform satisfaction and perspective differed between the eight students who showed significant NCL improvement and the other students who did not show as much significant improvement.

Keywords: Cybersecurity, Competition, Gamification, Student satisfaction

Recommended Citation: Grech, B.P., (2026). Evaluating Eleven Online CTF Platforms for Undergraduate Cybersecurity Competition Preparation *Cybersecurity Pedagogy and Practice Journal.* v5(n2) pp 78-103. DOI# https://doi.org/10.62273/FWOS1592

Evaluating Eleven Online CTF Platforms for Undergraduate Cybersecurity Competition Preparation

Brandon P. Grech

1. INTRODUCTION

An inaugural 'Competitions in Cybersecurity' course was developed and launched in Fall 2024 at a Christian institution of higher education in the Southeast region of the United States of America. Eighteen students passed this course. Throughout this course, students practiced within eleven available online cybersecurity CTF (Capture-the-Flag) or similar learning websites. Near the end of the semester, students participated in the National Cyber League Individual and Team Games. Besides the registration payment for the National Cyber League, which was covered by the institution, all other websites were free and accessible to the students. After students participated in each online platform during class and outside of class, each student completed an assessment form and answered questions regarding ease of access, platform technical difficulties, enjoyable experiences, and the effectiveness and applicability of the platform in preparation for the National Cyber League.

1.1 National Cyber League

The National Cyber League (NCL) is an online competition that is open to college students within the United States of America. The NCL also allows U.S. high schools to participate as well; however, the primary audience is at the collegiate level. The NCL consists of nine skill categories: open source intelligence, cryptography, password cracking, log analysis, network traffic analysis, forensics, web application exploitation, scanning, and enumeration and exploitation. The NCL consists of an Individual Game and a Team Game every semester. Each game is 56 hours long and typically starts on Friday (1 p.m. Eastern Time Zone) and ends on Sunday (9 p.m. Eastern Time Zone). The Team Game is typically hosted online two weeks after the Individual Game. The Team Game allows up to seven students to compete together. Registration for the NCL was $35 per student in Fall 2024; however, it has since been raised to $45 per student. Registration includes access to the NCL Gym, Practice Game, Individual Game, and Team Game. The NCL has been shown to be effective in preparing students for the workforce (Zeichick, 2024). Participation within the NCL has been growing. In Fall 2018, 2,450 students competed in the NCL Individual Game (National Cyber League, 2018). In Fall 2024, 4,585 students competed in the NCL Individual Game (National Cyber League, 2024a). The NCL Individual Game shows an increase of over 87% between Fall 2018 and Fall 2024.

The NCL does not have a maximum number of students that may participate from a specific institution (National Cyber League, n.d.-a). Other competitions, such as the Collegiate Cyber Defense Competition (CDCC) and Collegiate Penetration Testing Competition (CPTC), only allow one team from an institution to compete during the competition. CDCC allows for one team of eight competitors with four alternates (National Collegiate Cyber Defense Competition, n.d.). CPTC allows for one team of six competitors with two alternates (Collegiate Penetration Testing Competitions, n.d.). The National Cyber League does not have a limit on how many individuals can compete during the NCL Individual Games. The NCL also does not have a limit on how many different teams from the same institution may compete during the NCL Team Game. The NCL provides scalability and more opportunities for students to compete without having roster spots taken by other peers and classmates.

The NCL ties into other educational frameworks, such as the NSA Centers of Academic Excellence in Cyber Defense (CAE-CD) and the NIST NICE Workforce Framework for Cybersecurity (NICE Framework) Work Roles. The NCL provides a detailed outline of how the nine skill categories (mentioned above) align with thirty-six NSA CAE-CD Knowledge Units (National Cyber League, 2024b). The NCL also provides a detailed outline of how the NCL's nine skill categories align with thirty-five NICE Framework Work Roles (National Cyber League, 2021) as each NICE Framework Work Role has between two – nine NCL skill categories supporting each work role.

1.2 Goals of This Paper

By analyzing the assessments of each student's responses to each platform, this research looks to gain a better understanding of how students believe each experience was and if it was applicable in preparing for the National Cyber

League. This research also aims to identify if positive trends and significant improvements in national rankings were seen after students participated in this course and the eleven CTF websites. Ultimately, this research aims to help institutions assess which of these practice websites may help their students improve within the National Cyber League. Specifically, the research questions are as follows:

- What are the students' perspectives of each Capture-the-Flag (CTF) website?
- Was there a significant improvement in the National Cyber League found within students after participating in each CTF website?
- What student perspective differences are found between students who showed significant growth and those who did not?

This paper will begin by addressing the first question by sharing the survey results of all eighteen students regarding each CTF website. Additionally, this paper will also share significant improvements seen in National Cyber League Individual Game performances after students completed this course. Lastly, this paper will share the survey results of those students who showed significant growth after taking this course and any differences between these students and the remaining students.

1.3 Contributions of This Paper

This research is focused on sharing student experiences across eleven available online CTF platforms in preparation for the National Cyber League. Over 500 United States institutions of higher education participate in the National Cyber League each semester (National Cyber League, 2025); however, little research exists discussing how students are preparing for these competitions. This research aims to show institutions examples of freely available CTF websites that may be a good selection to utilize for NCL preparation. This research will also share student feedback that discusses which CTF websites students did not find as valuable as other websites.

1.4 Structure of This Paper

This research paper contains eight sections. Section 1 is the introduction. Section 2 discusses the methodology. Section 3 shares the course schedule. Section 4 contains the responses of each website. Section 5 discusses the improvement seen in National Cyber League performances. Section 6 compares the assessments of those who showed significant improvement with those who did not. Section 7 is the conclusion. Section 8 contains references.

2. METHODOLOGY

This research utilized an experiential, quantitative research design where students were introduced to a new online CTF platform each week to practice within. At the conclusion of the week, each student completed a four-question Likert-style assessment reflecting on their experiences. The four questions were:

(Q1) Do you agree it was easy to get enrolled and start practicing?
(Q2) Do you agree there were platform-related technical difficulties?
(Q3) Do you agree it was enjoyable?
(Q4) If you competed in the NCL Individual or Team Game before, do you agree this practice site is applicable to prepare for the NCL Games?

Each question had the available choices: Strongly Disagree, Disagree, Neither Agree nor Disagree, Agree, and Strongly Agree. Each choice was assigned a score of 1 – 5 as follows: Strongly Disagree (1), Disagree (2), Neither Agree nor Disagree (3), Agree (4), and Strongly Agree (5). The average of all responses was calculated. If a student did not respond, a 'No Response' is indicated and is not considered within the average.

This experiential cycle repeated eleven times throughout the semester with a new online CTF platform each week. Students also competed within the National Cyber League Individual Game near the end of the semester and again the following semester. Student performances were measured to determine whether participation within this course led to National Cyber League Individual Game performance increases compared to prior to taking this course. Figure 1 illustrates how Kolb's Experiential Learning Theory (Kolb, 1984) was applied in this research study.

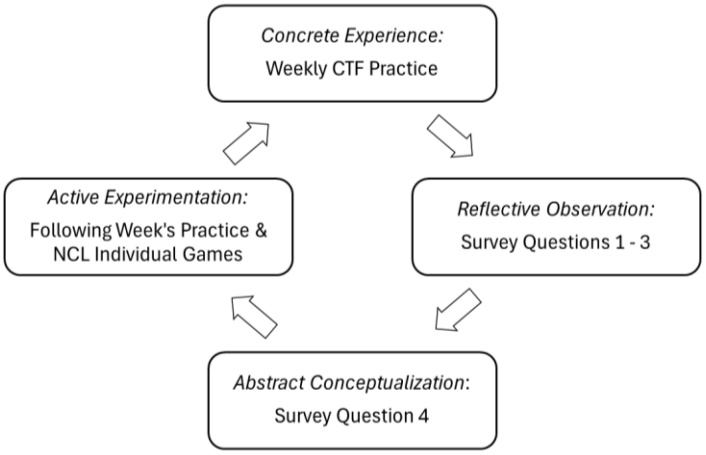


Figure 1. Application of Kolb's Experiential Learning Theory to Weekly CTFs

3. COURSE STUDENTS AND SCHEDULE

This section shares the schedule, tempo, and unexpected schedule changes of the 'Competitions in Cybersecurity' course.

3.1 Course Students

This inaugural course consisted of eighteen undergraduate students pursuing an undergraduate degree in cybersecurity at a Christian institution of higher education in the Southeast region of the United States of America. This course was a major elective that students could select; however, no students were required to enroll in this course. Students ranged from undergraduate sophomores to undergraduate seniors, as the only prerequisite for this course was a 100-level Linux course. Eleven of the eighteen students competed in the National Cyber League Individual Game in the previous semester. All eighteen students were traditional, in-person, undergraduate students who, at the time, had not yet gained full-time employment in a cybersecurity-related position.

3.2 CTF Practice Website Schedule

Each week, students practiced within an online CTF website and completed an assessment of their experiences. This course had in-person 75-minute classes each Tuesday and Thursday during the Fall 2024 semester. A majority of the students' time in class was spent working individually or in groups on each practice site; however, students spent even more time working on these practice sites outside of the class period. The schedule of the online CTF websites utilized is below.

Course Week	CTF Preparation Platform
Week 0	316ctf
Week 1	CTFlearn
Week 2	Bandit
Week 3	Natas
Week 4	picoGym
Week 5	247CTF
Week 6	Hacker101 CTF
Week 7	Root Me
Week 8	NCL Gym
Week 9	RingZer0 CTF
Week 10	Defend the Web

Table 1. CTF Practice Website Schedule

3.3 CTF Competition Schedule

Students also competed in six competitions throughout the semester. The first four competitions were utilized as further preparation for the National Cyber League Individual and Team competitions. The dates of each competition are below. Students had the option of PatriotCTF or ASIS CTF Quals as they were during the same week; however, all students chose to participate in PatriotCTF hosted online by George Mason's cybersecurity club. The official dates of the NSA Codebreaker Challenge were September 16th, 2024 – January 17th, 2025; however, the 'Competitions in Cybersecurity' course students were assigned to complete as much as they could within one week (October 8 – 14, 2024). Exploring experiences within the four non-NCL competitions as preparation for the National Cyber League is out of scope for this research and may be explored within future research.

Course Week	Dates	Competition
Week 1	Aug 31 – Sep 4, 2024	CISA ICS CTF 2024
Week 2	Sep 6 – 8, 2024	CSAW CTF Quals
Week 4	Sep 20 – 22, 2024	PatriotCTF
Week 7	Oct 8 – 14, 2024	NSA Codebreaker Challenge
Week 9	Oct 25 – 27, 2024	NCL Individual Game
Week 11	Nov 8 – 10, 2024	NCL Team Game

Table 2. CTF Competition Schedule

The 'Competitions in Cybersecurity' course students were also assigned a final team project where students in groups of three created their own CTF competition with various categories and custom challenges. An in-class demonstration of each project occurred during Week 14 of the course, which included a live demo showcasing various challenges being solved. Exploring the submissions of each team project is also out of scope for this research; however, students shared positive feedback regarding creating their own CTF competition from scratch during their presentations.

3.4 Unexpected Schedule Adjustments

During the semester in which the 'Competitions in Cybersecurity' course was being held, Hurricane Helene impacted the Southeastern United States. This natural disaster cancelled in-person classes for this course on October 1, 2024 and October 3, 2024. These two cancelled in-person classes were during Week 6. Fall Break was not cancelled; therefore, students did not have class on October 10 (as planned). To adjust for Hurricane Helene, only one in-person class day (instead of two) was devoted to Hacker101 CTF and Root Me. The NCL Gym was already scheduled for only one day due to Fall Break. Students were given extensions as needed to ensure enough time was dedicated to each preparation site outside of class.

4. ASSESSMENT RESULTS

This section shares a description of each of the CTF websites. The averages of each CTF's assessment results are found near the end of this section. The individual response scores related to the four questions answered after completing each CTF practice site are found in the appendices:

(Q1) Do you agree it was easy to get enrolled and start practicing?

(Q2) Do you agree there were platform-related technical difficulties?

(Q3) Do you agree it was enjoyable?

(Q4) If you competed in the NCL Individual or Team Game before, do you agree this practice site is applicable to prepare for the NCL Games?

4.1 316ctf

During Week 0, students participated in 316ctf. 316ctf is a persistent and growing CTF website created by Anderson University (SC) and the faculty member responsible for creating the 'Competitions in Cybersecurity' course. 316ctf is intended for middle-school and high-school students to explore categories such as Password Cracking, Cryptography, Open Source Intelligence, Web, and Network Analysis; however, it is open to everyone. The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix A.

4.2 CTFlearn

During Week 1, students participated in CTFlearn. CTFlearn claims to be the most beginner-friendly way to learn cybersecurity (CTFlearn, n.d.). CTFlearn has been utilized in previous research and was noted to be accessible (Albaladejo-González, et al., 2025); however, this research disagrees with this claim as many students within this course claimed to have technical difficulties within the CTFlearn platform. Prior research states CTFlearn has pedagogical content related to Reverse Engineering, Cryptography, Web Vulnerabilities, Binary Exploitation, and Forensics and Networking (Votipka, 2021) while additional research states CTFlearn consists of challenges related to Software Security, Reverse Engineering, Cryptography, Exploitation, Forensics, and Web Security (Lazarov, 2023); however, this research shows that students did not find this content enjoyable. The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix B.

4.3 Bandit

During Week 2, students participated in Bandit. Bandit is a wargame created by the OverTheWire community. OverTheWire claims Bandit is aimed at absolute beginners to learn Unix/Linux basics (OverTheWire, n.d.). Bandit has been criticized for being "too public" due to having walkthroughs

easily accessible (Ruff & Giacobe, 2022). Bandit has also been used to assist with launching a cybersecurity club by showcasing the different Linux skill levels of students (Piazza & Olmsted, 2015). Bandit has also been utilized by undergraduate students at a polytechnic institute that did not have a course covering the usage of the Linux terminal (Winters, 2020). The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix C.

4.4 Natas

During Week 3, students participated in Natas. Natas is another wargame created by the OverTheWire community. OverTheWire suggests Natas for learning web security after playing the Bandit wargame (OverTheWire, n.d.). The Natas platform has been effective as an introduction to hacking at collegiate hacking clubs (Radu & Thomas, 2015). Natas, and the previously mentioned Bandit, have also been utilized by faculty as additional content for students during cybersecurity labs (Singh et al., 2020). The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix D.

4.5 picoGym

During Week 4, students participated in picoCTF's picoGym. The picoCTF platform is a computer security education program created by Carnegie Mellon University (picoCTF, n.d.). The picoGym is available on-demand which hosts prior picoCTF event challenges and other challenges. Throughout the year, picoCTF has various events that are only available during the event. The picoGym has been utilized at other institutions to improve cybersecurity education (Ken et al., 2025). Writeups for some picoGym challenges are also publicly available (Leka, 2023). The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix E.

4.6 247CTF

During Week 5, students participated in 247CTF. 247CTF is a continuous security competition that offers challenges in various cybersecurity categories (247CTF, n.d.). The 247CTF platform has been utilized by institutions of higher education as one of the first steps towards building a competent CTF team (Goetgheluck et al., 2024). The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix F.

4.7 Hacker101 CTF

During Week 6, students participated in Hacker101 CTF. The Hacker101 CTF is another free website that allows people to play and learn cybersecurity skills (Hacker101, n.d.). Hacker101 CTF has been utilized to assist with preparing future bug bounty hunters (Cuevas et al., 2022). The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix G.

4.8 Root Me

During Week 7, students participated in Root Me. Root Me is another platform that allows people to learn computer security skills such as web security, network security, and reverse engineering (Paiva et al., 2023; Root Me, n.d.). The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix H.

4.9 NCL Gym

During Week 8, students participated in the NCL Gym. The NCL Gym contains challenges from previous NCL competitions. The NCL Gym is typically open throughout the semester to students after they have paid and registered for the National Cyber League (National Cyber League, n.d.-b). During the Fall 2024 semester, the NCL Gym was open between August 19 – December 13 (National Cyber League, 2024c). Students noted that a majority of the NCL Gym challenges were the same as the previous semester and had minimal changes between semesters. The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix I.

4.10 RingZer0

During Week 9, students participated in RingZer0's Team online CTF (RingZer0, n.d.). RingZer0's CTF has been modeled by graduate institutions teaching cybersecurity (Knight et al., 2020). The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix J.

CTF Platform	Q1	Q2	Q3	Q4
316ctf	4.72	1.78	4.39	4.11
CTFlearn	2.61	4.83	2.17	3.47
Bandit	4.33	1.89	4	3.53
Natas	4.61	1.72	4.22	4.44
picoGym	4.47	1.82	4.18	4.2
247CTF	4.43	2	3.57	3.83
Hacker101	4.13	2.19	3.75	3.71
Root Me	3.39	3.5	3.39	3.24
NCL Gym	4.61	1.39	4.28	4.47
RingZer0	4.25	2.12	3.47	3.44
Defend the Web	4.35	1.88	4	3.88

Table 3. Comparison of Practice Site Based on Course Order

4.11 Defend the Web

During Week 10, students participated in Defend the Web (Defend the Web, 2024). After the course, around early May 2025, the Defend the Web's home page claimed to be on hiatus due to running costs and personal commitments (Defend the Web, 2025). The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix K.

4.12 Comparing Each Eleven CTFs

Table 3 shows each of the eleven CTFs' average for each question in order of the course schedule.

The charts below show the data from all eighteen students ordered from highest to lowest regarding each question one through four.

In Figure 2, the average scores of responses regarding Question 1 'Do you agree it was easy to get enrolled and start practicing' are shown. The platforms 316ctf, NCL Gym, and Natas received a 4.6 or higher regarding easiness of enrolling and getting started. The majority of platforms scored an average of 4.0 or higher. The two platforms that showed enrollment and starting concerns were Root Me and CTFlearn.

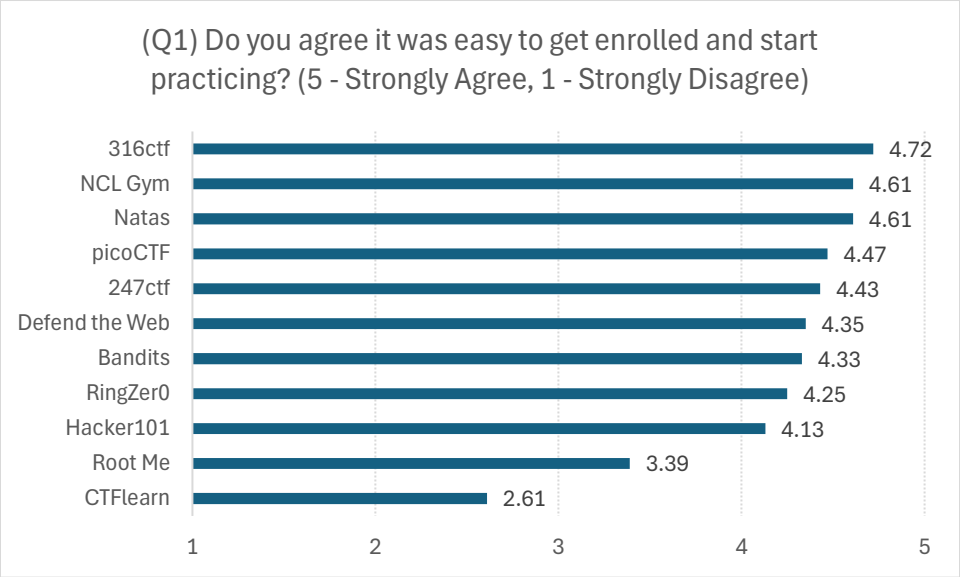


Figure 2. Comparison of Question 1 Averages Sorted Highest to Lowest (All Students)

In Figure 3, the average scores of responses regarding Question 2 'Do you agree there were platform-related technical difficulties' are shown. The students indicated there were technical difficulties within both CTFlearn and Root Me. Nearly all students strongly agreed there were technical difficulties within CTFlearn. The remaining nine platforms showed minimal technical difficulties.

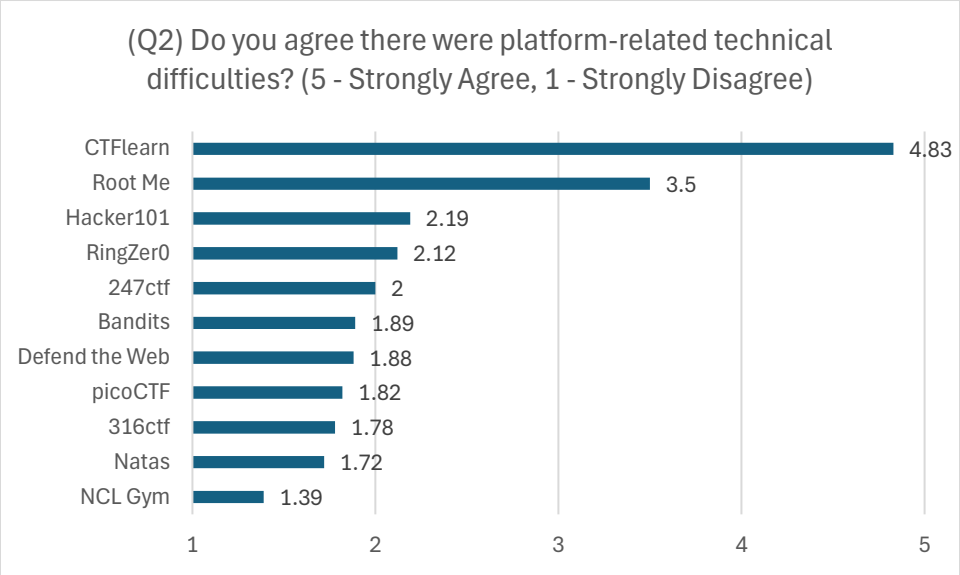


Figure 3. Comparison of Question 2 Averages Sorted Highest to Lowest (All Students)

In Figure 4, the average scores of responses regarding Question 3 'Do you agree it was enjoyable' are shown. Six of the eleven platforms scored a minimum of 4.0. These include 316ctf, NCL Gym, Natas, picoCTF, Defend the Web, and Bandit. The least enjoyable platforms were the same two that had platform-related difficulties (CTFlearn and Root Me).

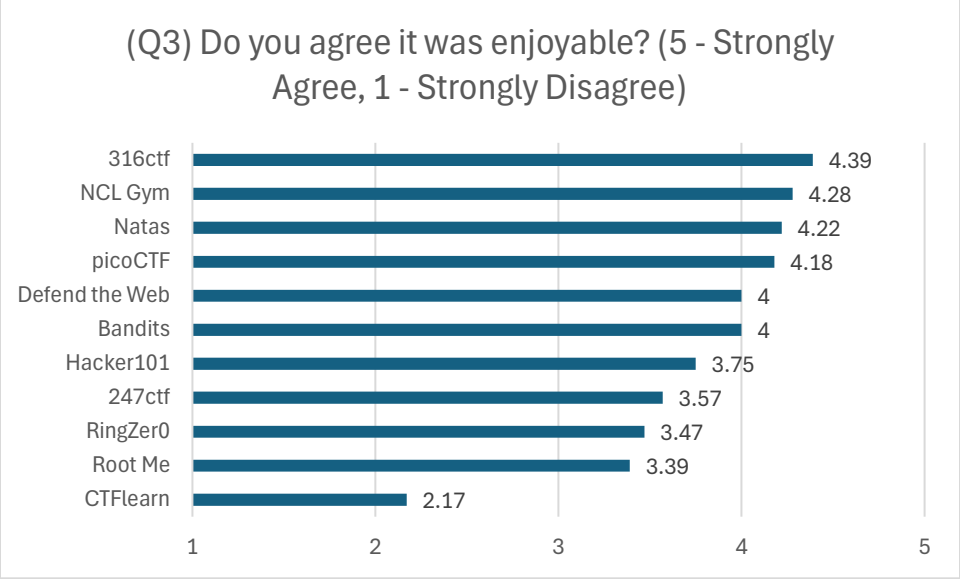


Figure 4. Comparison of Question 3 Averages Sorted Highest to Lowest (All Students)

In Figure 5, the average scores of responses regarding Question 4 'If you competed in the NCL Individual or Team Game before, do you agree this practice site is applicable to prepare for the NCL Games' are shown. Four of the eleven platforms scored a minimum of 4.0. These include NCL Gym, Natas, picoCTF, and 316ctf. The platform RingZer0 scored the second-lowest score and joined CTFlearn and Root Me as the three least agreed upon in preparing for the NCL Games.

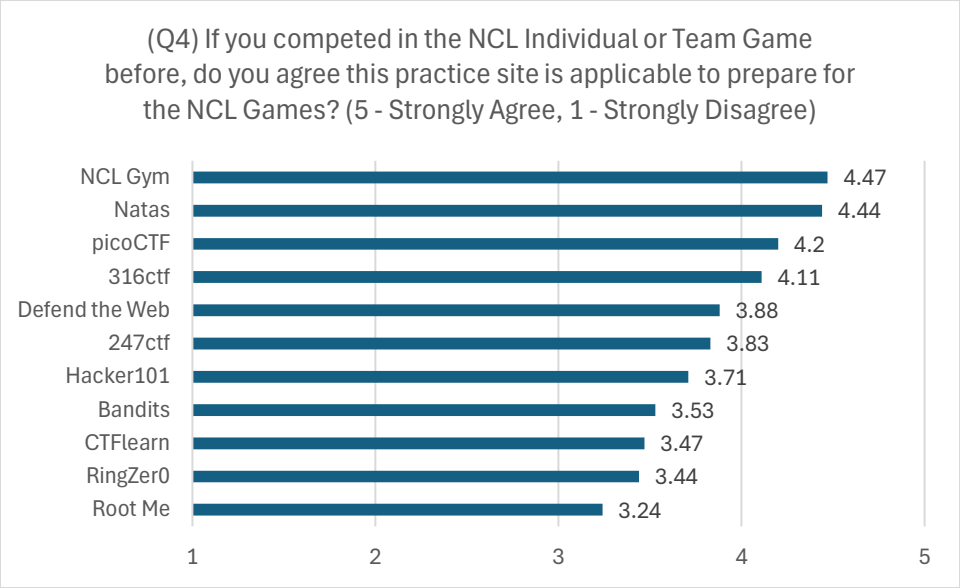


Figure 5. Comparison of Question 4 Averages Sorted Highest to Lowest (All Students)

5. IMPROVEMENTS IN NCL COMPETITION

Out of the 18 students who successfully completed this course in Fall 2024, 11 competed in the National Cyber League Individual Game in Spring 2024 (the semester prior to the course being offered).

During the course's semester, 17 students competed in the Fall 2024 National Cyber League Individual Game. During the following semester, 13 students competed in the Spring 2025 National Cyber League Individual Game.

The statistics below share how many students placed in each tier. These numbers are non-cumulative; for example, a student ranked in the Top 100 is not also considered in the Top 500. A few students who did not participate were ineligible to compete due to graduating before the competition(s).

This research data shows that prior to taking the course, zero course students placed in the Top 50, four placed in the Top 100, and an additional two placed in the Top 500. Within the semester, immediate improvements were made as one student placed in the Top 50, three placed in the Top 100, and two placed in the Top 500. During the following semester, the largest improvement occurred, as four students placed in the Top 50 and an additional four students placed in Top 500. This data and positive trend are shown below.

NCL Ind. Ranking	Spring 2024	Fall 2024	Spring 2025
Top 50	**0**	**1**	**4**
Top 100	**4**	**3**	**0**
Top 500	**2**	**2**	**4**
Top 1000	2	2	1
Outside Top 1000	3	9	4
Did Not Participate	7	1	5

Table 4. NCL Individual Rankings Before, During, and After the Course

6. COMPARISON OF STUDENT ASSESSMENT

Out of the 18 students who successfully completed this course, eight showed significant improvement. A student is considered to have shown significant improvement if they placed in the Top 500 during or after completing the 'Competitions in Cybersecurity' course and if they improved their ranking in Fall 2024 and/or Spring 2025 compared to their Spring 2024 placement, if available (prior to the course).

As previously stated, eleven students competed in the Spring 2024 NCL Individual Game and seven did not. These students may have competed in a previous NCL Team Game or an even earlier NCL Individual Game which would fulfill the requirement to answer Question 4. Placing in the Top 500 is a challenging feat, as over 4,600 students competed in the Spring 2025 National Cyber League Individual Game. The National Cyber League awards the individuals who place in the Top 500 in the standard bracket during Individual Games by mailing them a physical challenge coin as an award. This research will now explore if these eight students' experiences differ from the remaining ten students who did not make such a significant improvement and did not place in the Top 500 in any of their NCL Individual competitions. The eight students who made significant improvements (Top 500 and improved their ranking, if available) will be referred to as 'Group A' and the remaining ten students will be referred to as 'Group B'.

6.1 Question 1 Comparison

The table and figure below visually represent the differences between Group A and Group B's experiences getting enrolled and beginning practicing. The data has been ordered from highest to lowest based on Group A's experience. Group A showed much more dissatisfaction with CTFlearn compared to Group B.

CTF Platform	Group A	Group B
picoGym	4.86	4.2
Natas	4.75	4.5
NCL Gym	4.75	4.5
316ctf	4.63	4.8
247CTF	4.6	4.33
Bandit	4.38	4.3
Defend the Web	4.29	4.4
RingZer0	4.29	4.22
Hacker101	4	4.25
Root Me	3.13	3.6
CTFlearn	1.63	3.4

Table 5. Question 1 Comparison Between Group A and Group B (Table)

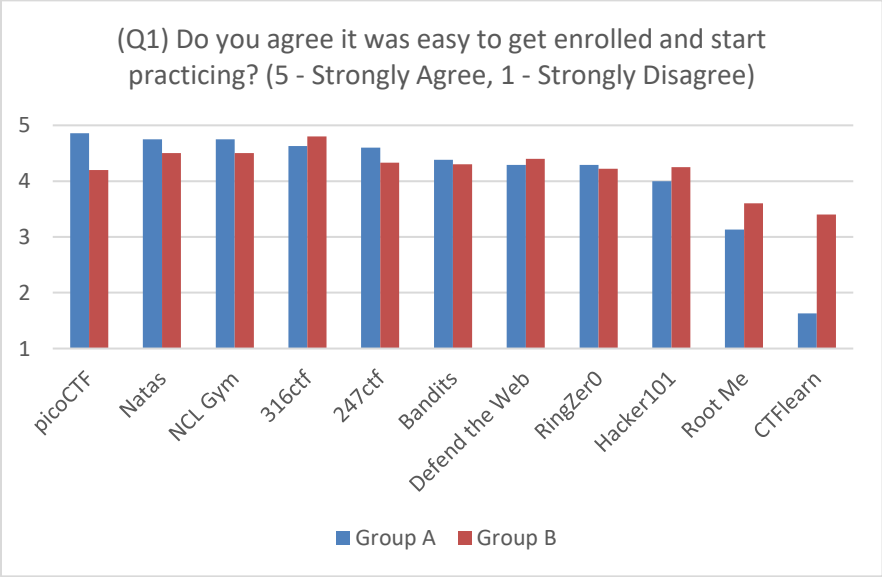


Figure 6. Question 1 Comparison Between Group A and Group B (Bar Chart)

CTF Platform	Group A	Group B
CTFlearn	5	4.7
Root Me	3.75	3.3
Hacker101	2.13	2.25
Defend the Web	2	1.8
RingZer0	2	2.2
Bandit	1.63	2.1
247CTF	1.6	2.22
316ctf	1.38	2.1
picoGym	1.29	2.2
Natas	1.25	2.1
NCL Gym	1.13	1.6

Table 6. Question 2 Comparison Between Group A and Group B (Table)

6.2 Question 2 Comparison

The table and figure below visually represent the differences between Group A and Group B's experiences with platform-related technical difficulties. The data has been ordered from highest to lowest based on Group A's experience.

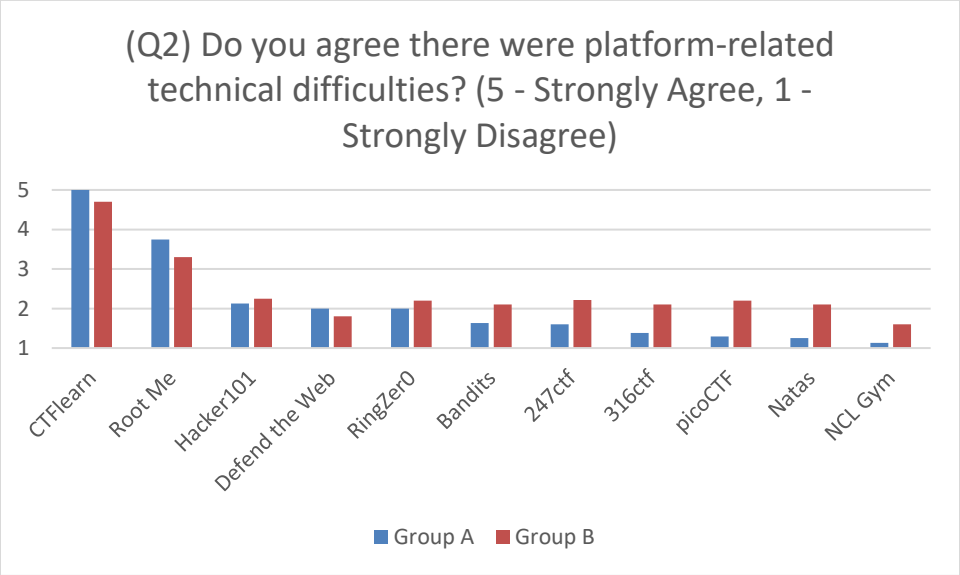


Figure 7. Question 2 Comparison Between Group A and Group B (Bar Chart)

6.3 Question 3 Comparison

The table and figure below visually represent the differences between Group A and Group B's enjoyment of each platform. The data has been ordered from highest to lowest based on Group A's experience.

CTF Platform	Group A	Group B
picoGym	4.57	3.9
Natas	4.5	4
NCL Gym	4.5	4.1
316ctf	4.25	4.5
RingZer0	4	3.1
247CTF	4	3.33
Hacker101	3.88	3.63
Bandit	3.88	4.1
Defend the Web	3.71	4.2
Root Me	3.5	3.3
CTFlearn	2	2.3

Table 7. Question 3 Comparison Between Group A and Group B (Table)

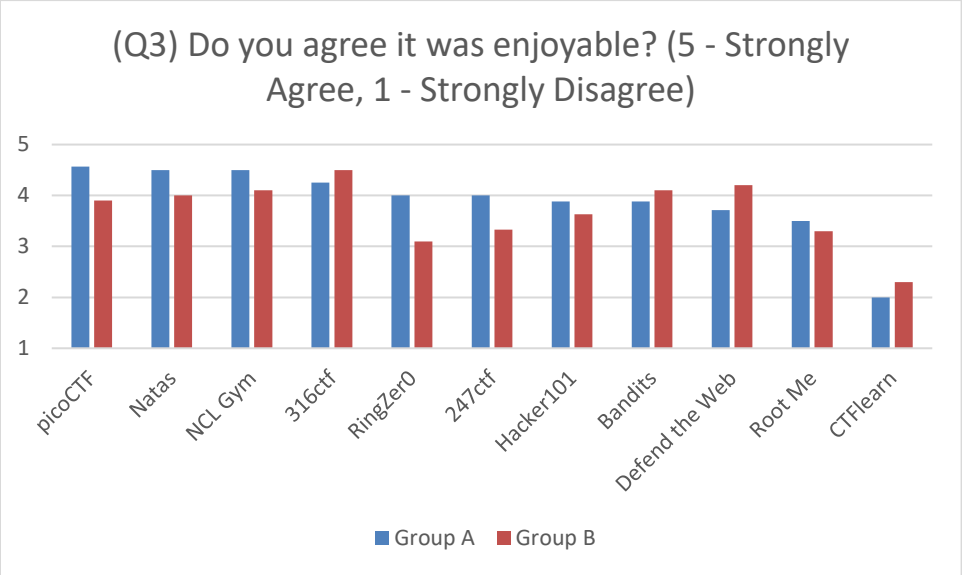


Figure 8. Question 3 Comparison Between Group A and Group B (Bar Chart)

6.4 Question 4 Comparison

The table and figure below visually represent the differences between Group A and Group B's opinions on whether the platform is applicable in preparing for the National Cyber League. The data has been ordered from highest to lowest based on Group A's experience.

CTF Platform	Group A	Group B
Natas	4.88	4
picoGym	4.57	3.88
NCL Gym	4.5	4.44
316ctf	4.25	4
247CTF	4.2	3.57
Defend the Web	4.14	3.7
Hacker101	3.88	3.5
RingZer0	3.86	3.11

Bandit	3.5	3.56
CTFlearn	3.25	3.67
Root Me	3.13	3.33

Table 8. Question 4 Comparison Between Group A and Group B (Table)

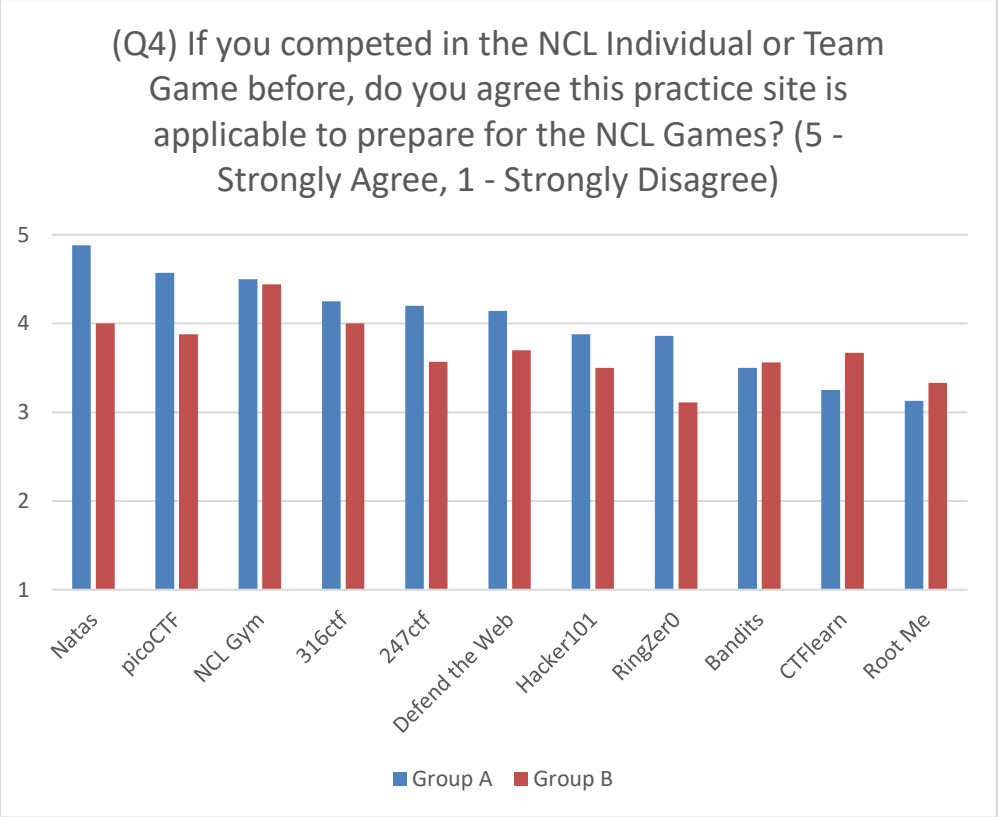


Figure 9. Question 4 Comparison Between Group A and Group B (Bar Chart)

7. CONCLUSION

This research has shown that a cybersecurity course dedicated to competitions in cybersecurity can have a significant positive impact on students' placements in National Cyber League competitions. This research has discovered that students who showed significant improvement believe that Natas, picoGym, and the NCL Gym were the most applicable in preparing students for the National Cyber League Games. The same students found the same three platforms (picoGym, Natas, and NCL Gym) were also the most enjoyable. The platforms 316ctf and 247CTF also had a 4 or higher in both enjoyability and applicability to the NCL Games, according to students who showed significant improvement (Group A). It is also of interest that Group A's top four enjoyable platforms were in order picoGym, Natas, NCL Gym, and 316ctf; however, Group B's top four enjoyable platforms were the same in reverse order with 316ctf followed by NCL Gym, Natas, then picoGym. Students also found platform-related technical problems and enrollment/starting issues in the CTFlearn and Root Me platforms. The Defend the Web platform is currently inaccessible since this inaugural course's research. Faculty members, cybersecurity competition coaches, and students who are looking for enjoyable and applicable platforms for the National Cyber League should strongly consider looking at picoGym, Natas, and the NCL Gym and explore the remaining platforms within this research as additional potential preparation sites for the National Cyber League. This research can and should be replicated at other schools within a course or a cybersecurity club to identify if similar significant improvements are found with National Cyber League individual performances. The findings of this research have been applied to the following year's second iteration of the 'Competitions in Cybersecurity' at this institution, which is being offered in Fall 2025.

8. REFERENCES

247CTF. (n.d.). *Home*. https://247ctf.com/

Albaladejo-González, M., Nespoli, P., Gómez Mármol, F., & Ruipérez-Valiente, J. A. (2025). A multimodal and adaptive gamified system to improve cybersecurity competence training. *Cluster Computing, 28*(9). https://doi.org/10.1007/s10586-025-05264-6

Collegiate Penetration Testing Competition. (n.d.). *Overview*. RIT ESL Global Cybersecurity Institute. https://cp.tc/overview

CTFlearn. (n.d.). *Learn cybersecurity*. https://ctflearn.com/

Cuevas, A., Hogan, E., Hibshi, H., & Christin, N. (2022). Observations from an online security competition and its implications on crowdsourced security. *arXiv*. https://doi.org/10.48550/arXiv.2204.12601

Defend the Web. (2024). *An interactive cyber security platform*. Wayback Machine. https://web.archive.org/web/20241013223256/https://defendtheweb.net/

Defend the Web. (2025). *Goodbye*. Wayback Machine. https://web.archive.org/web/20250507233154/https://defendtheweb.net/

Goetgheluck, Y., Mernit, S., & Pereira, J. (2024). Gamification of IT for training in information systems management. *Colloque International Game Evolution 2024*. https://hal.science/hal-04579392/

Hacker101 CTF. (n.d.). *Home*. HackerOne. https://ctf.hacker101.com/

Ken, C. L., Juremi, J., Alizadeh, S., & Sulaiman, S. (2025). Enhancing cybersecurity education through gamified learning and capture the flag (CTF) platform. *Communications in Computer and Information Science*, 69–82. https://doi.org/10.1007/978-3-031-98003-9_6

Knight, G. S., Leblanc, S., Devendorf, E., & Shuck, M. (2020). Design it, build it, defend it: Using cyber exercises in the education of cyber forces. In G. Austin (Ed.), *National cyber emergencies: The return to civil defence* (Chapter 13). Routledge.

Kolb, D. A. (1984). *Experiential learning: Experience as the source of learning and development*. Prentice-Hall.

Lazarov, W., Stodulka, T., Schafeitel-Tähtinen, T., Helenius, M., & Martinasek, Z. (2023). Interactive environment for effective cybersecurity teaching and learning. *Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES)*, 1–9. https://doi.org/10.1145/3600160.3605007

Leka, C. (2023). *CTFLib / A collection of writeups of capture-the-flag challenges for beginners*. University of Piraeus. https://dione.lib.unipi.gr/xmlui/handle/unipi/15290

National Collegiate Cyber Defense Competition. (n.d.). *NCCDC rules and requirements*. National CCDC. https://www.nationalccdc.org/rules.htm

National Cyber League. (n.d.-a). *Rules of conduct*. Cyber Skyline. https://nationalcyberleague.org/competition/rules

National Cyber League. (n.d.-b). *Competition*. https://nationalcyberleague.org/competition

National Cyber League. (2018). *Leaderboard: Fall 2018*. Cyber Skyline. https://cyberskyline.com/hosted_events/ncl-fall-2018

National Cyber League. (2021). *NCL category alignment: How NCL cybersecurity skill categories align to the NIST NICE cybersecurity work roles and CompTIA certifications*. Cyber Skyline. https://drive.google.com/file/d/1sC-eeRyclL0qV-mOf-hB1kqu3SmXZZZc/view

National Cyber League. (2024a). *Leaderboard: Fall 2024*. Cyber Skyline. https://cyberskyline.com/hosted_events/ncl-fall-2024

National Cyber League. (2024b). *How NCL skill categories align to the NSA Centers of Academic Excellence in Cyber Defense (CAE-CD) Knowledge Units (KUs)*. Cyber Skyline.

https://drive.google.com/file/d/1Z8khijDbNRC_wOx5Z89re03Rns82UcWD/view

National Cyber League. (2024c). *Competition*. Wayback Machine. https://web.archive.org/web/20241206033728/https://nationalcyberleague.org/competition

National Cyber League. (2025). *Cyber power rankings: Spring 2025*. Cyber Skyline. https://cyberskyline.com/data/power-ranking/spring-2025-national

OverTheWire. (n.d.). *Wargames*. https://overthewire.org/wargames/

Paiva, J. C., Queirós, R., & Gasiba, T. (2023). Sifu reloaded: An open-source gamified web-based cybersecurity awareness platform (short paper). *Proceedings of the 4th International Computer Programming Education Conference (ICPEC), 112*, 5:1–5:8. https://doi.org/10.4230/OASIcs.ICPEC.2023.5

Piazza, M., & Olmsted, A. (2015). Herding cats: How to launch a cyber security club in an academic setting. *International Journal for Information Security Research, 5*(2), 559–564. https://doi.org/10.20533/ijisr.2042.4639.2015.0064

picoCTF. (n.d.). *Home*. Carnegie Mellon University. https://picoctf.org/

Radu, A., & Thomas, S. L.. *Organising monkeys or how to run a hacking club*. University of Birmingham. https://inaradu.com/publications/Organising_Monkeys.pdf

RingZer0. (n.d.). *RingZer0 team online CTF*. https://ringzer0ctf.com/

Root Me. (n.d.). *CTF all the day*. https://www.root-me.org/en/Capture-The-Flag/CTF-all-the-day/

Ruff, M., & Giacobe, N. A. (2022). Leveraging browser-based virtual machines to teach operating system fundamentals. *Journal of The Colloquium for Information Systems Security Education, 9*(1), 7. https://doi.org/10.53735/cisse.v9i1.150

Singh, M., Singh, P., & Kumar, P. (2020). An analytical study on cross-site scripting. *2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)*, 1–6. https://doi.org/10.1109/iccsea49143.2020.9132894

Votipka, D., Zhang, E., & Mazurek, M. L. (2021). Hacked: A pedagogical analysis of online vulnerability discovery exercises. *2021 IEEE Symposium on Security and Privacy (SP)*, 1268–1285. https://doi.org/10.1109/sp40001.2021.00092

Winters, T. (2020). *Evaluation of effective teaching materials and techniques for software security engineering* [Master's thesis, Worcester Polytechnic Institute]. https://digital.wpi.edu/downloads/k643b3960

Zeichick, D. (2024). Confidence and competence: The impact of National Cyber League participation on career development in cybersecurity. *Journal of Computing Sciences in Colleges, 39*(10), 40–47. http://ccsc.org/publications/journals/SW2024.pdf

APPENDIX A

316ctf Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	5	2	4	4
Student02	5	1	4	4
Student03	5	1	5	4
Student04	5	5	5	5
Student05	5	1	4	3
Student06	5	2	4	4
Student07	5	1	5	5
Student08	5	2	5	4
Student09	5	2	4	4
Student10	4	4	4	4
Student11	5	1	5	4
Student12	5	1	5	4
Student13	4	2	4	3
Student14	4	2	4	3
Student15	4	1	4	5
Student16	4	2	4	5
Student17	5	1	4	5
Student18	5	1	5	4
Average	4.72	1.78	4.39	4.11

APPENDIX B

CTFlearn Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	2	5	1	4
Student02	3	5	4	4
Student03	2	5	3	3
Student04	2	5	2	4
Student05	4	5	1	3
Student06	1	5	2	2
Student07	5	5	2	4
Student08	4	5	4	No Response
Student09	4	5	3	4
Student10	4	3	4	4
Student11	1	5	1	3
Student12	1	5	2	4
Student13	3	5	2	4
Student14	4	4	2	4
Student15	1	5	2	3
Student16	1	5	2	4
Student17	2	5	1	2
Student18	3	5	1	3
Average	2.61	4.83	2.17	3.47

APPENDIX C

Bandit Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	5	2	4	4
Student02	5	1	4	4
Student03	4	2	5	4
Student04	5	1	4	3
Student05	5	1	4	3
Student06	4	4	3	3
Student07	5	2	4	5
Student08	4	2	5	No Response
Student09	3	1	4	4
Student10	5	5	3	3
Student11	4	1	3	3
Student12	5	1	5	4
Student13	4	2	4	5
Student14	3	2	4	3
Student15	4	1	4	2
Student16	5	2	4	4
Student17	4	1	4	3
Student18	4	3	4	3
Average	4.33	1.89	4	3.53

APPENDIX D

Natas Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	5	1	4	5
Student02	5	1	4	5
Student03	4	2	4	4
Student04	5	1	4	4
Student05	5	5	4	3
Student06	5	1	5	5
Student07	5	1	5	4
Student08	4	2	4	No Response
Student09	3	1	2	4
Student10	5	4	4	3
Student11	5	2	5	5
Student12	5	2	5	5
Student13	4	1	5	5
Student14	4	2	4	No Response
Student15	4	1	4	4
Student16	5	1	4	5
Student17	5	1	4	5
Student18	5	2	5	5
Average	4.61	1.72	4.22	4.44

APPENDIX E

picoGym Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	4	2	4	4
Student02	5	1	5	5
Student03	4	2	4	4
Student04	5	1	4	4
Student05	4	2	3	3
Student06	5	1	5	5
Student07	5	1	5	4
Student08	4	2	4	No Response
Student09	4	2	4	4
Student10	5	4	4	4
Student11	No Response	No Response	No Response	No Response
Student12	5	1	4	4
Student13	4	2	5	4
Student14	4	2	4	No Response
Student15	5	1	4	4
Student16	5	2	4	5
Student17	5	1	5	5
Student18	3	4	3	4
Average	4.47	1.82	4.18	4.2

APPENDIX F

247CTF Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	4	2	2	4
Student02	5	1	5	5
Student03	4	2	4	4
Student04	5	1	4	4
Student05	4	1	3	3
Student06	No Response	No Response	No Response	No Response
Student07	5	1	3	3
Student08	4	2	4	No Response
Student09	4	4	3	3
Student10	5	5	3	4
Student11	No Response	No Response	No Response	No Response
Student12	5	1	4	4
Student13	4	2	4	4
Student14	4	2	4	No Response
Student15	4	2	4	4
Student16	5	2	3	4
Student17	No Response	No Response	No Response	No Response
Student18	No Response	No Response	No Response	No Response
Average	4.43	2	3.57	3.83

APPENDIX G

Hacker101 Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	No Response	No Response	No Response	No Response
Student02	5	1	4	4
Student03	4	2	4	3
Student04	4	2	3	4
Student05	4	1	4	3
Student06	3	2	4	4
Student07	5	2	4	4
Student08	4	2	4	No Response
Student09	4	4	3	4
Student10	5	3	4	3
Student11	4	1	4	4
Student12	4	3	3	4
Student13	3	2	4	4
Student14	4	2	3	No Response
Student15	4	4	4	3
Student16	5	2	4	4
Student17	4	2	4	4
Student18	No Response	No Response	No Response	No Response
Average	4.13	2.19	3.75	3.71

APPENDIX H

Root Me Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	3	2	4	4
Student02	5	4	5	4
Student03	4	3	2	2
Student04	3	4	2	2
Student05	4	5	4	3
Student06	5	4	4	4
Student07	4	4	4	4
Student08	4	2	4	No Response
Student09	4	3	2	3
Student10	4	4	4	4
Student11	1	5	2	2
Student12	2	4	4	2
Student13	4	2	5	4
Student14	4	2	4	4
Student15	3	4	4	3
Student16	4	2	3	3
Student17	1	5	1	3
Student18	2	4	3	4
Average	3.39	3.5	3.39	3.24

APPENDIX I

NCL Gym Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	5	3	4	5
Student02	5	1	5	5
Student03	4	2	5	4
Student04	5	1	5	5
Student05	4	1	2	3
Student06	4	1	4	3
Student07	5	1	4	5
Student08	4	2	4	No Response
Student09	4	2	4	5
Student10	5	1	5	5
Student11	5	1	5	5
Student12	5	1	4	5
Student13	4	2	4	3
Student14	4	2	4	3
Student15	5	1	5	5
Student16	5	1	5	5
Student17	5	1	4	5
Student18	5	1	4	5
Average	4.61	1.39	4.28	4.47

APPENDIX J

RingZer0 Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	4	2	4	4
Student02	4	2	4	4
Student03	No Response	2	4	4
Student04	5	1	4	3
Student05	4	2	1	3
Student06	5	2	5	4
Student07	5	2	4	4
Student08	4	2	4	No Response
Student09	4	2	1	1
Student10	4	4	2	3
Student11	No Response	No Response	No Response	No Response
Student12	5	1	4	4
Student13	4	4	4	4
Student14	4	2	4	4
Student15	4	1	4	4
Student16	4	2	4	4
Student17	4	2	3	3
Student18	4	3	3	2
Average	4.25	2.12	3.47	3.44

APPENDIX K

Defend the Web Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	4	2	4	4
Student02	5	1	5	5
Student03	4	2	4	4
Student04	5	1	3	3
Student05	5	1	5	3
Student06	4	2	3	4
Student07	5	1	5	5
Student08	5	2	4	4
Student09	3	2	4	3
Student10	5	3	5	3
Student11	No Response	No Response	No Response	No Response
Student12	5	1	4	4
Student13	4	4	2	4
Student14	4	2	4	4
Student15	4	1	4	4
Student16	4	4	4	4
Student17	4	1	4	4
Student18	4	2	4	4
Average	4.35	1.88	4	3.88

Federated Learning and Edge Computing for Privacy-Preserving Real-Time Predictive Maintenance in Industrial IoT Systems

Kiran Kumar Vejendla
vejendlakiran@gmail.com

Kyong (Jin) Chang
changkyong@cityu.edu

Brian Maeng
maengjooyol@cityu.edu

Sherin Aly
alysherin@cityu.edu

City University of Seattle
Seattle,WA 98121

Abstract

This paper presents a framework involving Federated Learning (FL) and Edge computing (EC) (FL-EC) to achieve privacy-preserving and real-time predictive maintenance in the Industrial Internet of Things (IIoT) systems. FL reduces the privacy risk by training machine learning models on local edge-devices without the transmission of sensitive data, whereas EC executes data nearer to the source decreasing latency and increasing responsiveness. The FL-EC framework demonstrates high accuracy, F1-score, and recall compared to traditional centralized models, establishing its utility for real-time fault detection. Scalability is also provided by the framework, making the system effective to support different and heterogeneous edge devices. FL-EC helps to solve the most important problems of traditional IIoT systems by maintaining data confidentiality and limiting latency. The research also contrasts FL-EC with the available literature and shows that it can be applied practically in the automotive and oil and gas industry as well as in industries where real-time monitoring and maintenance are essential. The results indicate that FL-EC has the potential to achieve significant cost-saving and efficiency improvement in industry. The future research must aim at improving federated learning algorithms, solving the non-IID data problem, and enabling the optimization of edge devices to be better performing and customized, which will guarantee a wider application in IIoT settings.

Keywords: Federated Learning, Edge Computing, Predictive Maintenance, IIoT, Privacy-Preserving, Real-Time Fault Detection

Recommended Citation: Vejendla, K., Chang, K., Maeng, B., Aly, S. (2026). Federated Learning and Edge Computing for Privacy-Preserving Real-Time Predictive Maintenance in Industrial IoT Systems. *Cybersecurity Pedagogy and Practice Journal.* v5(n2) pp 104-116. DOI# https://doi.org/10.62273/GPYS1669

Federated Learning and Edge Computing for Privacy-Preserving Real-Time Predictive Maintenance in Industrial IoT Systems

Kiran Kumar Vejendla, Kyoung (Jin) Change, Brian Maeng and Sherlin Aly

1. INTRODUCTION

The Industrial Internet of Things (IIoT) has transformed how industries oversee and control equipment, making it possible to shift current maintenance approaches based on conventional maintenance tools to more dynamic ones, including predictive maintenance (PM) (Naidoo & Sibanda, 2024). Predictive maintenance involves real-time information collected through interconnected sensors and is used to predict equipment malfunction prior to its happening to enable an organization to maximize its operations, minimize downtimes and increase its output (Civerchia et al., 2017). Nevertheless, the increasing dependency on centralized machine learning models in IIoT systems causes a number of acute problems, in particular, with privacy, latency, and scalability.

Conventional predictive maintenance systems face major challenges hindering their adoption in IIoT settings. To begin with, there is a privacy issue because vast amounts of sensitive operational information need to be sent between the edge devices to centralized servers to process information, which puts pressure on risks of data leakage and breaches of data protection laws, including the General Data Protection Regulation (GDPR) (Ali et al., 2021). Besides, centralized systems can create delays in real-time fault detection and decision-making since it requires time to send the data and make predictions at a central point. The delay can be incredibly problematic especially in those industries that demand instant responses, like automotive or oil and gas (Bhaskaran et al., 2020). Lastly, being scalable is also a major concern since centralized systems are not able to cope with large volumes of data that are produced by a wide range of diverse and geographically dispersed devices and equipment in industrial settings. Such constraints underscore the need to have a more decentralized, efficient and privacy preserving predictive maintenance in IIoT.

To address these challenges, this study proposes a combination of Federated Learning (FL) and Edge Computing (EC) that can facilitate privacy-protected real-time predictive maintenance in IIoT systems (Alshkeili et al., 2025). Federated Learning (FL) is a machine learning method that is decentralized, which enables the local training of models without requiring the transfer of raw data to central servers. FL can suppress transmission of data, as well as lower the risk of privacy by aggregating locally trained models (Beltrán et al., 2023). Conversely, EC processes data nearer to the source that is at the edge of the network, hence, greatly reducing latency and makes it possible to provide fault detection analysis in real-time. FL combined with EC is the promising solution to addressing the intrinsic issues of privacy, latency and scalability of traditional IIoT predictive maintenance systems (Liu et al., 2024).

This model provides the assurance that sensitive information is held on peripheral devices, and it complies with the stringent privacy rules and, nevertheless, allows the worldwide compilation of models to make correct predictions of faults. Furthermore, the capacity of edge computing to deal with real-time data processing at the edge prevents the reduction in the latency of the decision-making process, providing a more reactive method of predictive maintenance. Therefore, the integrated FL-EC framework can overcome the main shortcomings of centralized systems, namely the ability to scale to larger heights, ensuring security, and enabling maintenance of IIoT processes in real-time. This research addresses the following key questions:

1. How effectively does Federated Learning (FL) mitigate privacy risks while maintaining model accuracy?
2. How does the combination of FL and Edge Computing (EC) affect the process of anomaly detection and feature extraction in sensor data to predictive maintenance of IIoT?
3. What is the benefit of the proposed decentralized structure in terms of detecting faults in real time by learning temporal dependencies in industrial time-series data as well as the issue of privacy, latency, and scalability?
4. Is the edge computing/FL combination less latent than centralized predictive maintenance systems?

5. To what extent can the proposed framework be scaled when evaluated with a variety of industrial configurations with different types of machines and sensor configurations?

Using the advantages of Federated Learning and Edge Computing, this study will discuss a new form of predictive maintenance that will effectively solve the weaknesses of centralized systems. The suggested framework is an excellent chance to address the challenge of privacy, latency, and scalability of the traditional IIoT systems, which have become a part of the current process of digital transformation of industries. With the ongoing development of IIoT and the proliferation of this device type, this combined FL-EC model can potentially become a key enabler of safer, more efficient and reliable predictive maintenance systems and create operational gains and cost reductions in a variety of industries.

Previous Research Overview

The Industrial Internet of Things (IIoT) is important in facilitating predictive maintenance (PdM) by constantly tracking machines and equipment to identify the initial indicators of possible failure. Recent innovations have focused on changing the conventional reactive maintenance methods to more effective predictive-based maintenance methods based on real-time data that are detected by different sensors in the industrial setting (Hafeez et al., 2021). An example of this, Civerchia et al. (2017) discussed the application of IIoT to advanced predictive maintenance describing a system applicable to a real-world electricity power plant. Their solution showed a notable decrease in downtimes and a better reliability of the equipment based on real-time sensor data. Nevertheless, one of the remaining issues is the sheer volume of information produced by IIoT devices that makes it difficult to process and transmit them to cloud-based systems.

Federated Learning (FL) has become a promising approach to privacy-aware machine learning in IIoT environments. FL supports collaborative model training across edge devices without transferring their raw operational data to a central repository. Fan et al. (2022) proposed a privacy-preserving aggregation scheme that combines secret sharing with the Paillier cryptosystem, an additive homomorphic public-key encryption method that permits selected arithmetic operations on encrypted values without first revealing the underlying plaintext. This combination is intended to protect model updates and reduce exposure to model-update reconstruction or inference attacks while controlling communication and computation costs. Odeh et al. (2024) subsequently introduced asynchronous FL for mobile-edge IIoT ecosystems, addressing device heterogeneity and network delay in decentralised training.

The edge computing (EC) has also become a part of the IIoT as it allows processing data nearer to the data generation point, minimizing the time and transmission expenses. Hafeez et al. (2021) emphasized the role of EC in addressing the high real-time demands of IIoT applications and how it is used in predictive maintenance in particular. They talked about the use of EC to handle the processing of large volumes of sensor data, decrease load on cloud infrastructure, and enhance the speed of decision-making. Besides, Liu et al. (2024) introduced a federated learning-based edge computing system that integrates the processing capabilities of edge nodes with the privacy-insurance characteristics of FL to be able to process data efficiently and provide security. This integration will be of particular importance in IIoT environments where the reduction of latency and the real-time performance are the primary considerations.

The combination of FL and EC are compatible and can help address the problems of IIoT-based predictive maintenance. By combining those two technologies, it is possible to train models in a decentralized manner, but at the same time, make sure that data privacy is not violated, and processing does not take too much time. Liu et al. (2024) examined the possibility of edge computing to minimize the latency by computing data on the device and introduced a frame of devices selection and computation offloading to improve the federated learning process further. Their architecture proves the cooperation of FL and EC to handle the huge volumes of data IIoT devices produce and provide more effective and more privacy-aware predictive maintenance solutions.

Privacy remains a concern in IIoT federated systems because adversaries may attempt to infer sensitive information from model updates. Fan et al. (2022) combined Practical Byzantine Fault Tolerance (PBFT), secret sharing, and Paillier-based encrypted aggregation to support fault-tolerant coordination when devices fail or behave maliciously. These mechanisms are designed to reduce exposure to reconstruction and tampering risks; however, their effectiveness depends on the assumed threat model, key management, and implementation details.

Although these are optimistic advances regarding federated learning and edge computing regarding IIoT-based predictive maintenance, a number of challenges still persist. Among the most prominent ones is that data in IIoT settings is not IID (Non-Independent and Identically Distributed) and, therefore, this aspect may adversely affect the functionality of federated learning models (Hongbin & Zhi, 2023). The other difficulty is that such systems are difficult to scale when used in large and heterogeneous industrial networks. More studies are required to come up with more efficient FL algorithms capable of addressing the challenges of non-IID data and still ensuring privacy and security. Moreover, it is necessary to have better strategies of device selection and computation offloading to make better use of edge computing resources and minimize the energy usage and latency of predictive maintenance systems (Liu et al., 2024).

As modern software architectures have shifted toward distributed, microservice-based, and cloud-native paradigms, Application Performance Monitoring (APM) has evolved from a reactive diagnostic capability into a fundamental operational requirement. Modern observability practices provide continuous runtime visibility into application behavior, enabling organizations to detect performance degradation, prevent service-level agreement (SLA) violations, optimize resource utilization, and maintain service reliability in increasingly complex distributed environments (Usman et al., 2022).

Research gap and incremental contribution. Existing studies demonstrate that FL and EC can be combined, but they frequently concentrate on one component of the problem. Fan et al. (2022) emphasise privacy-preserving aggregation, whereas Liu et al. (2024) emphasise edge resource selection and computation offloading. However, existing frameworks have largely overlooked the critical component of monitoring. This paper does not claim to introduce the first FL-EC architecture, a new cryptosystem, or a new aggregation optimiser. Its contribution is an application-specific design-science artifact and a unified empirical matrix that evaluates centralised and federated CNN/LSTM models, multiple aggregation strategies, a hybrid CNN-LSTM, secure versus non-secure exchange, latency, scalability, and PySyft-based distributed simulation for the same predictive-maintenance context. The novelty is therefore incremental and integrative: it shows how architectural, learning, and security choices interact rather than evaluating them in isolation in an enterprise context.

2. RESEARCH METHODOLOGY

This study adopted a mixed-methods methodology with an exploratory sequential design. It began with a qualitative phase, utilizing a literature review of existing frameworks, followed by a quantitative, experiment-based evaluation to construct and assess a privacy-aware, low-latency predictive-maintenance artifact for an IIoT setting. The procedure comprised four linked phases: (i) requirements and problem formalisation, (ii) framework design and development, (iii) experimental simulation and comparative evaluation, and (iv) performance, latency, scalability, and security-impact assessment.

Phase 1: Requirements and problem formalisation. A focused review of IIoT predictive-maintenance challenges was used to identify three operational requirements: local data confidentiality, real-time responsiveness, and scalability across heterogeneous edge clients. These requirements were translated into measurable criteria comprising accuracy, precision, recall, F1-score, latency, and communication overhead.

Phase 2: Framework design and development (artifact creation). The artifact was derived by mapping each operational requirement to an architectural mechanism. The privacy requirement led to local data retention, parameter-only exchange, and support for protected aggregation; the latency requirement led to edge-level preprocessing and inference; and the scalability requirement led to modular client, communication, orchestration, and aggregation functions. The designs reported by Fan et al. (2022) and Liu et al. (2024) were used as reference points, but the components were reorganised into a three-layer predictive-maintenance artifact and linked to a common comparative evaluation plan. This requirement-to-component mapping explains how the proposed framework was created and how each element relates to a stated research objective.

Phase 3: Experimental simulation and comparative evaluation. The framework was evaluated with the publicly available AI4I 2020 Predictive Maintenance Dataset from the UCI Machine Learning Repository. The observations were partitioned to represent multiple edge clients under decentralised conditions. Centralised baselines were compared with FL-EC

variants using Federated Averaging (FedAvg), Federated Proximal (FedProx), Federated Normalised Averaging (FedNova), and Federated Dynamic Regularisation (FedDyn). Fault-prediction architectures comprised a Convolutional Neural Network (CNN), a Long Short-Term Memory network (LSTM), and a hybrid CNN-LSTM model.

Phase 4: Performance, latency, scalability, and security-impact assessment. Classification performance was measured using accuracy, precision, recall, and F1-score. End-to-end latency incorporated local inference and model-update time in the centralised and edge-enabled configurations. Security overhead was examined by comparing secure and non-secure federated variants, while scalability was assessed by increasing the number of simulated clients and observing model stability and communication overhead.

The four-phase procedure links each design decision to an operational requirement and each research claim to a corresponding experimental measure. The framework is therefore presented as a systematically derived and empirically assessed integration artifact rather than as a purely conceptual architecture.

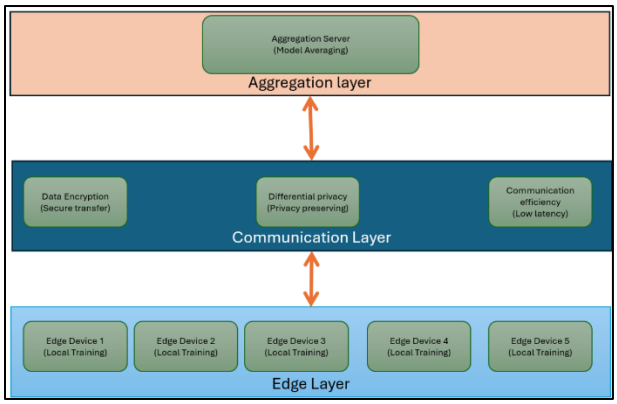


Figure 1: Proposed System Architecture

Figure 1 illustrates a three-layer FL–EC architecture. Edge devices perform local model training on IIoT data. The communication layer ensures secure, privacy-preserving, and low-latency parameter exchange. The aggregation layer combines local updates into a global model, enabling scalable, real-time, and privacy-aware predictive maintenance.

Dataset

In this research, the predictive maintenance Dataset (AI4I 2020) is taken as the main source of data. This is a dataset consisting of sensor data of industrial machines, and is applied to predictive maintenance. The UCI Machine learning Repository offers AI4I 2020 data, which covers the values of different operational parameters like temperature, vibration, and pressure that are crucial in identifying possible failures in the machine (Matzka., 2020).

There are 10,000 instances in the dataset, 22 features and a target variable as operational condition of the machine. The characteristics are the number of sensor readings and the target variable is the failure state of a machine (1) or the normal operating state of a machine (0). In predictive maintenance, the exercise is to model and predict whether the machine can fail or not basing on its past sensor reading. Such secondary data will be a source of valuable information that may be used to train machine learning models to predict equipment failures in industrial IoT (IIoT) systems, with no need to gather primary data.

Federated Learning Framework

The study uses Federated Learning (FL) to a dataset of AI4I 2020 to design a predictive maintenance model that is privacy-preserving. FL permits the distributed construction of machine learning models in many edge-computers, without communicating the original data. It is especially appropriate in IIoT, where privacy and data security are the primary priority.

The federation of learning model is a system where edge devices (connecting to various subsets of the dataset) use their data to train local models. This local model is combined by a central server to form a global model. FL framework guarantees that the sensitive information, including individual machine sensor readings is not stored on any remote server thereby protecting the privacy (Fan et al., 2022). In this study, we have applied a FedAvg (Federated Averaging) model-training algorithm. The most used federated learning algorithm is FedAvg in which every edge device trains a local model on their local data and transmits the model weights back to the central server. The server then sums up the model weights to generate the global model. This procedure minimizes the necessity of having physical access to the raw information but still making sure there is an ability to learn on the model using the aggregated insights across the devices.

Edge Computing Setup

The Edge Computing (EC) system applied in the study is aimed at reducing latency and enhancing the efficiency of the predictive maintenance architecture. EC provides edge processing of

data, which is nearer to the data source (i.e. the machines), thereby limiting the volume of data sent to the cloud and decision-making is faster. Here, the edge devices have the responsibility of doing preprocessing sensor data prior to transmitting aggregated models to the server where they learn further (Hafeez et al., 2021).

To conduct the secondary data analysis, EC is modeled by local data processing through the use of AI4I dataset. We do not transmit the raw sensor data to a central server, but instead simulate the operation of machine learning model training on local bits of data and combining them through the FL framework. This minimizes the overhead in communication and faster model updates are guaranteed.

Model Development
The main aim of the research project is to come up with a predictive maintenance model that is based on machine learning algorithms, capable of forecasting the possible failures of the industrial machines. The models that will be applied in this study are:

Convolutional Neural Network (CNN): CNNs are applied mainly to spatial feature extraction, thus it is more applicable to sensor data that could have spatial patterns. CNNs are able to identify anomalies in the machine sensors data by learning the features of the temperature, pressure, and vibration patterns that are usually predictive of a machine failure (Scarpa et al., 2018).
Long Sho
rt-Term Memory (LSTM): LSTMs are a type of Recurrent Neural Networks (RNN) which is very effective in the learning of temporal dependencies (Zhang et al., 2021). In this study, LSTMs are employed to forecast machine failures based on time-series information, which is necessary to model time-specked machine health data in IIoT settings.

Hybrid CNN-LSTM Model: This model is a combination of the two CNN and LSTM. The sensor data is extracted into features with CNN and modeled with LSTM to capture the time dependencies of features (Cheng et al., 2019). This hybrid methodology is especially applicable to predictive maintenance where it is possible to combine both spatial (e.g. unusual vibrations) and temporal (e.g. gradual wear and tear over time) patterns in machine behavior.

Evaluation Metrics
Model effectiveness was evaluated using standard classification and system-level measures. Accuracy is the proportion of all predictions classified correctly. Precision is the proportion of predicted failures that are genuine failures, whereas recall is the proportion of genuine failures detected by the model. The F1-score is the harmonic mean of precision and recall and is useful when balancing false alarms against missed failures. Latency is the elapsed time required to preprocess an observation, perform inference, and complete the relevant model-update operation. Scalability is assessed by examining whether performance and communication behaviour remain stable as the number of participating federated clients increases.

Experimental Setup
The section provides the description of the experimental set up in which the proposed FL-EC framework will be tested under controlled and reproducible conditions. The experiments were performed based on the AI4I 2020 Predictive Maintenance dataset consisting of 10,000 cases with 22 sensor-derived and operational features of the behavior of industrial machines. The binary target variable suggests normal functioning or failure and thus, the dataset can be used in fault prediction activities in IIoT.

Client Partition Strategy (IID / Non-IID)
In order to model a federated IIoT setup, the data was distributed among several virtual edge clients. Both non-IID and IID data distributions were taken into consideration. Non-IID partitions are used to simulate practical industrial environments in which machines run with varying loads and under varying conditions, and the data heterogeneity is introduced among clients.

Baselines
The FL-EC models were compared with centralised CNN and LSTM baselines. The federated environment considered Federated Averaging (FedAvg), which computes a data-weighted average of client updates; Federated Proximal (FedProx), which adds a proximal term to limit local-model drift; Federated Normalised Averaging (FedNova), which normalises client updates to account for unequal local work; and Federated Dynamic Regularisation (FedDyn), which uses dynamic regularisation to improve optimisation under heterogeneous data.

Hyperparameters and Training Configuration
All experiments were trained on fixed hyperparameters to ensure fairness. The federated training was done on several rounds where each client had a specified number of local

epochs in each round then model aggregation was done.

Evaluation Metrics and Latency Measurement

The measures of performance were through accuracy, precision, recall, and F1-score. Latency was determined as the end-to-end response time, including the local inference and model update latencies, which allowed straightforward comparison between centralized and FL–EC systems.

Proposed FL–EC Framework

The proposed FL-EC framework is an application-specific integration artifact for predictive maintenance; it is not presented as the first general FL-EC architecture. Its purpose is to organise local sensing, edge processing, protected parameter exchange, federated orchestration, and comparative evaluation within one reproducible workflow focused on privacy, latency, scalability, and fault-detection performance in an enterprise context where monitoring is highly required.

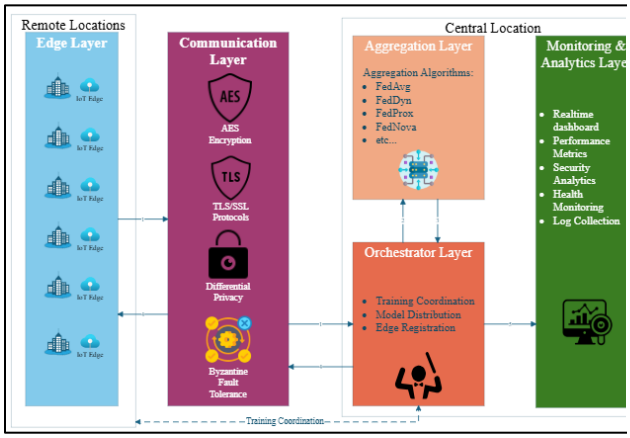


Figure 2: Proposed Federated Predictive Maintenance Framework

Figure 2 presents the end-to-end architecture. At the edge layer, IIoT devices or edge nodes acquire and preprocess operational observations, train local model copies, and perform local fault inference. Raw observations remain within the local client boundary; only model parameters or updates are prepared for transmission. This separation reduces routine raw-data movement and enables low-latency local decisions, although FL alone does not eliminate all information-leakage risks.

The communication layer connects the edge clients with the central orchestrator. It supports authenticated parameter transfer and, in the secure variant, protected aggregation or encrypted update exchange. These controls are intended to reduce unauthorised access and update reconstruction rather than to claim complete elimination of adversarial risk. Communication efficiency is evaluated because the additional protection may increase computation, payload size, or convergence time.

The aggregation and orchestration layer selects participating clients, coordinates training rounds, combines local updates using the selected federated optimiser, and redistributes the updated global model. In contrast with Fan et al. (2022), whose primary contribution is secure aggregation, and Liu et al. (2024), whose framework emphasises device selection and computation offloading, the present artifact centres on a unified predictive-maintenance comparison across model architectures, aggregation methods, security settings, latency, scalability, and monitoring. This integrative evaluation constitutes the principal contribution of the framework.

High-level algorithmic flow. (1) Initialise a global CNN, LSTM, or CNN-LSTM model and select the participating edge clients. (2) Each client preprocesses its local observations and trains a local model for the specified number of local epochs. (3) The client transmits only its model update, using the protected communication option when the secure variant is evaluated. (4) The orchestrator aggregates client updates using FedAvg, FedProx, FedNova, or FedDyn. (5) The updated global model is redistributed and the process repeats for the configured communication rounds. (6) The final model is evaluated through local inference, predictive metrics, latency, convergence behaviour, communication overhead, and client-scaling tests.

3. RESULTS AND ANALYSIS

The results are reported in distinct experimental stages to prevent values from different runs being compared as though they came from one configuration. The centralized baselines correspond to the standalone CNN, LSTM, and hybrid CNN-LSTM evaluations. The federated results then report mean performance for each model–algorithm combination across the simulated federated experiments, followed by pooled algorithm-level summaries, secure-versus-standard server effects, efficiency analysis, and the separate NetworkFed/PySyft evaluation. This ordering preserves the

experimental hierarchy and avoids mixing model-specific, pooled, and networked results.

Table 1. Centralized baseline model performance

Model	Acc.	Prec.	Rec.	F1
CNN	0.9465	0.9712	0.9465	0.9558
LSTM	0.9430	0.9718	0.9430	0.9537
Hybrid CNN-LSTM	0.9320	0.9708	0.9320	0.9465

Table 1 summarizes the centralized baseline results. CNN achieved the highest centralized accuracy (0.9465) and F1-score (0.9558), followed closely by LSTM with 0.9430 accuracy and 0.9537 F1. The hybrid CNN-LSTM remained strong but lower at 0.9320 accuracy and 0.9465 F1. These values establish the centralized reference points for the subsequent federated experiments.

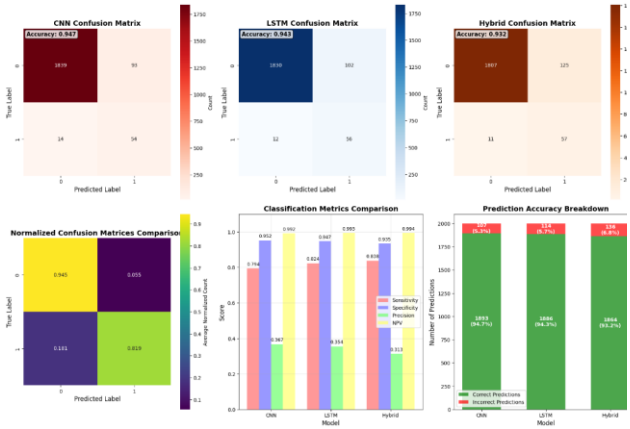


Figure 3. Centralized CNN, LSTM, and hybrid model confusion matrices and comparative performance

Figure 3 confirms the same ordering. CNN produced 1,839 true negatives and 54 true positives, LSTM produced 1,830 true negatives and 56 true positives, and the hybrid model produced 1,807 true negatives and 57 true positives. The comparative confusion matrices show that all three centralized models remain above 0.93 accuracy, while failure-class sensitivity is lower than overall accuracy because the underlying classification problem is imbalanced.

Federated simulation results were then evaluated across the four aggregation algorithms evaluated in the study: FedAvg, FedDyn, FedNova, and FedProx. Table 2 reports the mean model–algorithm values averaged across the relevant simulated distributions and server settings. These means must not be confused with the centralized baselines in Table 1 or with the pooled algorithm averages reported later.

Table 2. Federated model–algorithm mean performance

Configuration	Acc.	F1	Prec.	Rec.
CNN-FedAvg	0.5137	0.3585	0.3453	0.5137
CNN-FedDyn	0.5000	0.3333	0.2500	0.5000
CNN-FedNova	0.5179	0.3795	0.4318	0.5179
CNN-FedProx	0.5050	0.3424	0.2934	0.5050
Hybrid-FedAvg	0.5515	0.4296	0.4938	0.5515
Hybrid-FedDyn	0.4995	0.3345	0.2536	0.4995
Hybrid-FedNova	0.5056	0.3455	0.4093	0.5056
Hybrid-FedProx	0.5340	0.3954	0.4157	0.5340
LSTM-FedAvg	0.9456	0.9425	0.9554	0.9456
LSTM-FedDyn	0.4794	0.3223	0.2474	0.4794
LSTM-FedNova	0.9471	0.9453	0.9530	0.9471
LSTM-FedProx	0.9553	0.9545	0.9609	0.9553

Table 2 changes the interpretation of the federated results materially. The strongest configuration is LSTM-FedProx (accuracy 0.9553, F1 0.9545), followed by LSTM-FedNova (0.9471, F1 0.9453) and LSTM-FedAvg (0.9456, F1 0.9425). In contrast, CNN and hybrid federated configurations remain near 0.50-0.55 accuracy, and LSTM-FedDyn falls to 0.4794. The results therefore support an architecture-dependent conclusion: high federated performance is concentrated in LSTM with FedAvg, FedNova, or FedProx, rather than being a general property of every FL-EC model.

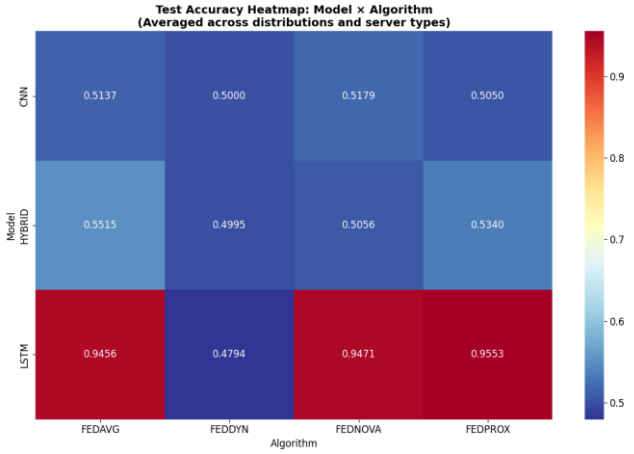


Figure 4. Federated test-accuracy heatmap by model and aggregation algorithm

Figure 4 visualizes the same model–algorithm means. The separation between LSTM and the CNN/hybrid models is pronounced, and FedDyn is the weakest algorithm for LSTM. LSTM-FedProx reaches 0.9553 test accuracy, whereas the strongest CNN and hybrid configurations remain at 0.5179 and 0.5515, respectively. This pattern demonstrates that federated performance depends strongly on the interaction between model architecture and aggregation algorithm.

Table 3. Pooled algorithm-level performance

Algorithm	Mean Acc.	Mean F1	Balance
FedAvg	0.6703	0.5769	0.6289
FedDyn	0.4929	0.3300	0.3915
FedNova	0.6569	0.5568	0.6172
FedProx	0.6648	0.5641	0.6126

Table 3 is a pooled algorithm-level summary, not a best-model table. FedAvg has the highest mean accuracy (0.6703) and balance score (0.6289), followed by FedProx and FedNova, whereas FedDyn is lowest at 0.4929 mean accuracy. The pooled means are substantially below the best LSTM values because they average over the weak CNN and hybrid runs shown in Table 2. The analysis also reports 95% accuracy confidence intervals of 0.649-0.691 for FedAvg, 0.489-0.497 for FedDyn, 0.636-0.678 for FedNova, and 0.644-0.686 for FedProx.

Security was evaluated as a pooled server-type effect across federated runs. This is another aggregation level and should not be compared directly with a single LSTM configuration. The pooled results show that secure operation produced only a small change in mean accuracy and recall while increasing mean precision.

Table 4. Secure versus standard federated server impact

Metric	Standard	Secure	Difference	Significant?
Accuracy	0.6231	0.6193	-0.0038	No
F1	0.5036	0.5103	+0.0066	No
Precision	0.4846	0.5170	+0.0323	Yes (p=0.044)
Recall	0.6231	0.6193	-0.0038	No

As shown in Table 4, secure aggregation reduced mean accuracy by only 0.0038 and changed F1 from 0.5036 to 0.5103. Precision increased from 0.4846 to 0.5170, with this difference statistically significant (p = 0.044), whereas the other metric differences were not significant. The supported interpretation is that the secure server setting did not materially degrade pooled predictive performance.

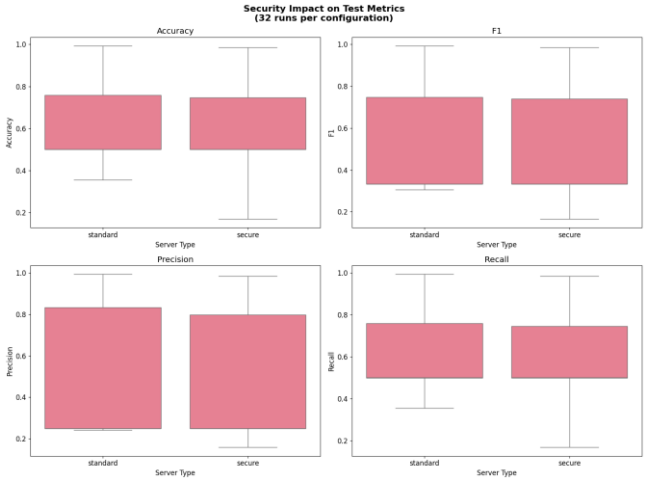


Figure 5. Security impact on accuracy, F1, precision, and recall across 32 runs per configuration

Figure 5 shows strongly overlapping standard and secure distributions for accuracy, F1, precision, and recall, consistent with the pooled statistics in Table 4. The modest precision shift is visible, but the overall distributions remain similar. This supports privacy-preserving aggregation with limited measured performance cost in the simulated experiments.

Real-time suitability is assessed using the efficiency analysis, which reports accuracy per minute for the leading model–algorithm configurations. This measure captures the predictive-performance-to-training-time trade-

off without treating efficiency as equivalent to classification accuracy or inference latency.

Table 5. Efficiency ranking based on accuracy per minute

Model	Algorithm	Score	Std. Dev.
LSTM	FedAvg	1.458	0.715
LSTM	FedNova	1.398	0.740
LSTM	FedDyn	1.394	0.513
LSTM	FedProx	0.794	0.344
CNN	FedDyn	0.257	0.088

Table 5 ranks LSTM-FedAvg highest on the reported efficiency measure (1.458), followed by LSTM-FedNova (1.398) and LSTM-FedDyn (1.394). This ranking is an efficiency measure and does not imply that FedDyn has the best predictive accuracy; Table 2 shows that LSTM-FedDyn accuracy is only 0.4794. Reporting the two measures separately is necessary because an efficiency ranking is not equivalent to a predictive-performance ranking.

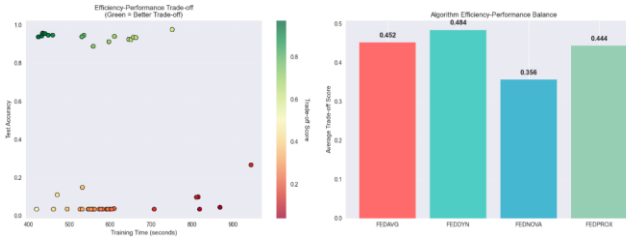


Figure 6. Efficiency-performance trade-off across federated configurations

Figure 6 further shows that computational efficiency and predictive accuracy are not interchangeable. High-accuracy configurations occupy a distinct region of the trade-off plot, while the algorithm-level trade-off score reflects the balance between runtime and performance. Consequently, the evidence supports configuration-aware efficiency assessment rather than a single universal latency advantage for FL-EC.

The NetworkFed/PySyft stage is reported separately from the 48-experiment simulation because it represents a different networked training condition and produces a distinct performance distribution. The networked analysis therefore focuses on the model–algorithm patterns observed in the corresponding experiment outputs rather than merging them with the simulated federated means.

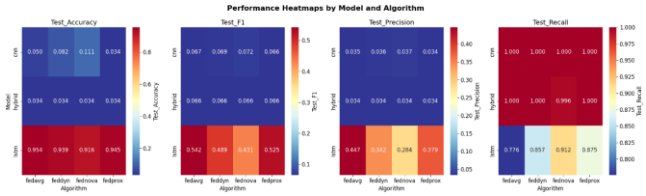


Figure 7. NetworkFed/PySyft performance heatmaps by model and aggregation algorithm

Figure 7 shows that, in the networked federated stage, LSTM test accuracy remains high across algorithms (approximately 0.916-0.954), whereas CNN and hybrid accuracies are much lower (approximately 0.034-0.111). The very high recall values for CNN and hybrid models occur alongside very low precision and accuracy, indicating a class-imbalance or prediction-bias effect rather than good overall classification. The networked evidence therefore reinforces the central result of the study: architecture and aggregation choice strongly condition federated predictive-maintenance performance.

Overall, the results do not support a blanket claim that FL-EC outperforms centralized learning for every model. Centralized CNN and LSTM are strong baselines, while federated LSTM with FedProx, FedNova, or FedAvg reaches comparable or slightly higher accuracy in the simulated experiments. Federated CNN and hybrid variants are substantially weaker, FedDyn is inconsistent across architectures, secure aggregation has little pooled performance cost, and the networked experiments remain configuration-sensitive. Taken together, these findings show that model-specific, pooled, and networked results must be interpreted within their respective evaluation settings.

Discussions, Limitations, and Future Directions

The concept of integrating Federated Learning (FL) and Edge Computing (EC) presents an interesting option to address urgent issues in the field of predictive maintenance in the Industrial Internet of Things (IIoT) related to privacy, latency, and scalability. FL can be decentralized to train models, where the data is kept at the edge devices and there is therefore a very minimal risk of data breaches. This will deal with the issue of privacy, which is key in the world of IIoT, where the data involved in operations can be very sensitive. Also, the EC component can process data locally, avoiding the transmission of data to centralized servers and greatly lowering the latency. This is essential in real time fault monitoring where delays will translate to

expensive downtime of equipment. Additionally, the FL-EC architecture is both extremely scalable and allows the processing of data in an efficient manner on a network of diverse devices that have different computing capacities. This scalability makes sure that as the number of edge devices increases the system will still work at an optimal level without affecting the accuracy or efficiency.

The FL-EC framework has various advantages over the traditional centralized systems when making comparisons. Centralized systems have the data of several devices transmitted to a central server to be processed and this presents a latency as well as privacy threat. Under FL and EC, model training is done directly on the devices and only model updates are transmitted thereby enhancing privacy maintenance (Haldikar et al., 2024). Besides, fault detection in FL-EC is also greatly improved because local processing of edge devices can provide faster decisions when compared to centralized systems where it could consume more time to upload and process data centrally (Liu et al., 2024). In general, FL and EC offer a more secure, fast, and scalable solution than traditional methods, which is why they are absolutely appropriate to IIoT-based predictive maintenance.

The findings are consistent with recent FL-EC research while adding an important qualification. Hafeez et al. (2021) focus on edge intelligence for data handling and predictive maintenance, Haldikar et al. (2024) examine FL and edge computing for real-time IIoT anomaly detection, Fan et al. (2022) concentrate on privacy-preserving aggregation, and Liu et al. (2024) emphasize edge resource selection and computation offloading. In the present experiments, centralized CNN and LSTM models remained strong, but federated performance varied sharply by architecture and optimizer. LSTM combined with FedProx, FedNova, or FedAvg produced the strongest federated results, while CNN and hybrid federated runs were markedly weaker. The contribution is therefore an integrated comparison that exposes the interaction between model architecture, aggregation, security setting, efficiency, and networked deployment rather than claiming universal FL-EC superiority.

The practical uses of FL-EC framework in the automobile, oil and gas, and manufacturing industries are enormous. An example of this is in the automotive industry, in which real-time predictive maintenance can be adopted to check the health of various vital parts of a vehicle, including engines and brakes, before they fail, and to improve the safety of the vehicle. Likewise, in the oil and gas sector, predictive maintenance can be used to monitor equipment like pumps, compressors, and turbines and determine their problems before the equipment becomes catastrophic (Fausing Olesen & Shaker, 2020). Companies that save lots of money in terms of repair and inefficiencies during operations, save much on the downtime and optimization of maintenance schedules. The fact that FL-EC framework has been able to offer real-time fault detection capability with great accuracy makes it a game changer in the industries where it is important to reduce operational interruptions. In addition, the privacy-saving aspect of FL takes care of the fact that sensitive industrial information is not revealed and that is crucial to those businesses that operate with proprietary technologies and regulatory requirements (Sarraf & Pal, 2022).

The evaluation has several limitations. First, the study uses a single public predictive-maintenance dataset and simulated or controlled federated clients, so generalization to different machines, sensing environments, and physical edge hardware remains unverified. Second, the large gap between LSTM and CNN/hybrid federated performance in Table 2 shows that results are sensitive to architecture, client data composition, and optimization conditions; repeated-seed and controlled IID/non-IID partition studies are therefore necessary. Third, edge devices have restricted memory, processing capacity, and network bandwidth, which may limit complex CNN-LSTM training. Model compression, lightweight architectures, adaptive client selection, and communication-efficient updates should therefore be evaluated together with accuracy. Finally, the efficiency analysis and NetworkFed results should be complemented by direct device-level measurements of processor time, memory use, transmitted bytes, energy consumption, and end-to-end latency on physical edge hardware.

Security, personalisation, and deployment feasibility. FL reduces routine raw-data centralisation but does not prevent poisoning, backdoor, Byzantine-update, model-inversion, or membership-inference attacks. Future evaluations should include authenticated clients, update clipping, anomaly screening, robust aggregation, secure aggregation, differential-privacy controls, and explicit adversarial testing. Per-device personalisation is also a useful extension: an edge client could fine-tune selected layers of the global model on its local operating profile, while retaining the shared model as a

common starting point. Such tuning may improve performance under heterogeneous machinery, but it should be controlled to avoid overfitting, unfair performance differences, and excessive energy or computational cost.

4. CONCLUSION

This study demonstrates the potential of an integrated Federated Learning and Edge Computing (FL-EC) framework for privacy-aware predictive maintenance in IIoT systems, while also showing that performance is strongly configuration-dependent. The centralized CNN and LSTM baselines achieved 0.9465 and 0.9430 accuracy, respectively. In the simulated federated experiments, LSTM-FedProx achieved the highest model-algorithm accuracy (0.9553), with LSTM-FedNova (0.9471) and LSTM-FedAvg (0.9456) close behind, whereas CNN and hybrid federated configurations remained near 0.50-0.55 accuracy. Pooled secure aggregation introduced only a small accuracy change (0.6231 to 0.6193) and increased precision from 0.4846 to 0.5170. The NetworkFed/PySyft results likewise favored LSTM and exposed weak CNN/hybrid behavior. The evidence therefore supports FL-EC as a promising privacy-preserving approach whose benefits depend on model architecture, aggregation algorithm, data partitioning, security configuration, and deployment conditions, rather than as an unconditional replacement for centralized learning.

Future work should reproduce all comparisons across multiple seeds and controlled IID/non-IID partitions, test the framework on real industrial data and physical edge devices, and measure energy, memory, communication payload, and end-to-end latency. Robust aggregation and adversarial evaluation are required to assess poisoning and inference risks. Resource-aware personalisation, model compression, and lightweight architectures should also be investigated to adapt the global model to individual machines without compromising scalability, fairness, or deployment feasibility.

5. REFERENCES

Ali, B., Gregory, M. A., & Li, S. (2021). Multi-access edge computing architecture, data security and privacy: A review. IEEE Access, 9, 18706-18721. https://doi.org/10.1109/ACCESS.2021.3053233

Alshkeili, H. M. H. A., Almheiri, S. J., & Khan, M. A. (2025). Privacy-Preserving Interpretability: An Explainable Federated Learning Model for Predictive Maintenance in Sustainable Manufacturing and Industry 4.0. AI, 6(6), 117. https://doi.org/10.3390/ai6060117

Beltrán, E. T. M., Pérez, M. Q., Sánchez, P. M. S., Bernal, S. L., Bovet, G., Pérez, M. G., Pérez, G. M., & Celdrán, A. H. (2023). Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges. IEEE Communications Surveys & Tutorials, 25(4), 2983-3013. https://doi.org/10.1109/COMST.2023.3315746

Bhaskaran, P. E., Chennippan, M., & Subramaniam, T. (2020). Future prediction & estimation of faults occurrences in oil pipelines by using data clustering with time series forecasting. Journal of Loss Prevention in the Process Industries, 66, 104203. https://doi.org/10.1016/j.jlp.2020.104203

Cheng, H., Xie, Z., Shi, Y., & Xiong, N. (2019). Multi-step data prediction in wireless sensor networks based on one-dimensional CNN and bidirectional LSTM. IEEE Access, 7, 117883-117896. https://doi.org/10.1109/ACCESS.2019.2937098

Civerchia, F., Bocchino, S., Salvadori, C., Rossi, E., Maggiani, L., & Petracca, M. (2017). Industrial Internet of Things monitoring solution for advanced predictive maintenance applications. Journal of Industrial Information Integration, 7, 4-12. https://doi.org/10.1016/j.jii.2017.02.003

Fan, H., Huang, C., & Liu, Y. (2022). Federated learning-based privacy-preserving data aggregation scheme for IIoT. IEEE Access, 11, 6700-6707. https://doi.org/10.1109/ACCESS.2022.3226245

Fausing Olesen, J., & Shaker, H. R. (2020). Predictive maintenance for pump systems and thermal power plants: State-of-the-art review, trends and challenges. Sensors, 20(8), 2425. https://doi.org/10.3390/s20082425

Hafeez, T., Xu, L., & Mcardle, G. (2021). Edge intelligence for data handling and predictive maintenance in IIOT. IEEE Access, 9, 49355-49371. https://doi.org/10.1109/ACCESS.2021.3069137

Haldikar, S. V., Kader, O. F. M. A., & Yekollu, R. K. (2024). Edge computing and federated learning for real-time anomaly detection in industrial Internet of Things (IIoT). In 2024 International Conference on Inventive Computation Technologies (ICICT) (pp. 1699-1703). Lalitpur, Nepal: IEEE. https://doi.org/10.1109/ICICT60155.2024.10544912

Hongbin, F., & Zhi, Z. (2023). Privacy-preserving data aggregation scheme based on federated learning for IIoT. Mathematics, 11(1), 214. https://doi.org/10.3390/math11010214

Liu, X., Dong, X., Jia, N., & Zhao, W. (2024). Federated learning-oriented edge computing framework for the IIoT. Sensors, 24(13), 4182. https://doi.org/10.3390/s24134182

Matzka, S. (2020). AI4I 2020 Predictive Maintenance Dataset UC Irvine Machine Learning Repository. https://doi.org/10.24432/C5HS5C

Naidoo, P., & Sibanda, M. (2024). Emerging trends and future directions of the industrial Internet of things. From Internet of Things to Internet of Intelligence, 91-110. https://doi.org/10.1007/978-3-031-55718-7_5

Odeh, J. O., Yang, X., Nwakanma, C. I., & Dhelim, S. (2024). Asynchronous privacy-preservation federated learning method for mobile edge network in industrial internet of things ecosystem. Electronics, 13(9), 1610. https://doi.org/10.3390/electronics13091610

Sarraf, G., & Pal, V. (2022). Privacy-Preserving Data Processing in Cloud: From Homomorphic Encryption to Federated Analytics. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(2), 735-706. https://doi.org/10.32628/IJSRCSEIT

Scarpa, G., Gargiulo, M., Mazza, A., & Gaetano, R. (2018). A CNN-based fusion method for feature extraction from sentinel data. Remote Sensing, 10(2), 236. https://doi.org/10.3390/rs10020236

Usman, M., Ferlin, S., Brunstrom, A., & Taheri, J. (2022). A survey on observability of distributed edge & container-based microservices. IEEE Access, 10, 86904-86919. https://doi.org/10.1109/ACCESS.2022.3193102

Zhang, J., Zeng, Y., & Starly, B. (2021). Recurrent neural networks with long term temporal dependencies in machine tool wear diagnosis and prognosis. SN Applied Sciences, 3(4), 442. https://doi.org/10.1007/s42452-021-04427-5

Perceived Usefulness of Password Complexity: A Methodology Framework

Kyle Herman
kherman@georgiasouthern.edu

Hayden Wimmer*
hwimmer@georgiasouthern.edu

School of Computing
Georgia Southern University
Statesboro, GA, USA

Abstract

This exploratory study investigates the factors influencing the adoption of complex passwords through the lens of the Technology Acceptance Model (TAM) by Davis (Davis, 1989). Data was collected via Qualtrics, and survey constructs were adapted from the pertinent Information Systems literature. Using Iterative Independent Variable Selection, Linear Regression and Partial Least Squares Structural Equation Modeling was then utilized to find significant constructs. The analysis found that Attitude towards Use, General Security Orientation, and Perceived Utility were significant predictors of behavioral intention to use complex passwords, explaining over 50% of the variance. The findings are supported by literature emphasizing the growing complexity of cyber security and the critical role of strong, unique passwords amid advancing threats. The study highlights the importance of user perceptions in secure behavior and contributes to understanding how theoretical frameworks like TAM can guide effective cyber security practices.

Keywords: Attitude Towards Use of Complex Passwords, Perceived Usefulness of Complex Passwords, Security Self-Efficacy, Cyber security, Linear Regression Analysis of Password Complexity.

Recommended Citation: Herman, K., Wimmer, H., (2026). Perceived Usefulness of Password Complexity: A Methodology Framework. *Cybersecurity Pedagogy and Practice Journal;* v2(n5) pp 117-131. DOI# https://doi.org/10.62273/OKIB1006

Perceived Usefulness of Password Complexity: A Methodology Approach

Kyle Herman and Hayden Wimmer

1. INTRODUCTION

Strong, complex passwords help safeguard individual users and their families, friends, and employers (Use Strong Passwords, n.d.). A compromised account can serve as a launch-pad for further attacks, exploiting trust within families or among colleagues in an organization. Gaining access to an email account or social media account enables bad actors to orchestrate scams and masquerade as the victim. In a corporate setting, a breached email account can be leveraged to spread misinformation, deceive high-value targets into revealing sensitive information, or trick them into clicking malicious links that steal credentials or install malware.

While Multi-Factor Authentication (MFA) has been widely adopted as a critical secondary layer of defense, passwords remain the primary authentication mechanism across most digital platforms. Furthermore, MFA systems often rely on primary passwords for account recovery, meaning a weak password can still compromise the entire security chain. Therefore, understanding what drives end-user adoption of complex passwords remains essential.

This study proposes an Iterative Independent Variable Selection (IIVS) method whereby we perform an exhaustive regression technique to determine the most important independent variables by reducing the regression equation to its significant independent variables. We confirm our method using Partial Least Squares (PLS) for latent variable calculation for each construct and model regression from the latent variable scores in SmartPLS 4. This work has the potential to advance information systems research by providing a new method for variable reduction and determining which factors are significant in adoption of technology.

Using Iterative Independent Variable Selection this exploratory study examines user's perceived usefulness of complex passwords. This work seeks to present a two-fold approach. We aim to determine the most salient factors for complex password adoption while also providing a methodological alternative to standard regression techniques.

2. LITERATURE REVIEW

Cybersecurity encompasses the resources, processes, and structures used to protect digital assets and cyberspace-enabled systems from unauthorized access, disruption, or exploitation (Craigen, Diakun-Thibault, et al., 2014). Similarly, the Cybersecurity and Infrastructure Security Agency (CISA) defines cybersecurity as the protection of networks, devices, and data from unauthorized access or criminal use while maintaining the confidentiality, integrity, and availability of information (What is Cybersecurity?, 2021). Within this broader security framework, passwords remain one of the most widely used mechanisms for user authentication. NIST Special Publication 800-132 defines a password or passphrase as a string of characters used to gain access to a restricted resource and establish user identity. Password strength is primarily influenced by length and randomness, particularly when passwords are used to derive cryptographic keys and must withstand offline guessing attacks (Turan, Barker, Burr, & Chen, 2010).

Although technical password requirements are important, their effectiveness is ultimately dependent on user behavior. Modern computing capabilities and automated password-cracking techniques increase the risk associated with weak, predictable, or reused credentials. NIST guidance emphasizes the importance of sufficiently long and unpredictable credentials, while CISA recommends unique passwords for individual accounts. However, enforcing increasingly complex password requirements does not necessarily produce more secure behavior. Instead, security requirements can create a tension between organizational security objectives and users' cognitive limitations.

Adams and Sasse (1999) demonstrated that when security mechanisms interfere with users' primary tasks, individuals frequently develop insecure coping strategies. These behaviors include writing passwords down, selecting predictable patterns, and reusing credentials across multiple accounts (Adams and Sasse, 1999). Herley (2009) further argued that users

often make security decisions based on the perceived costs and benefits of security practices, meaning that policies imposing substantial inconvenience may encourage users to circumvent them rather than comply (Herley, 2009).

Password reuse represents a particularly significant consequence of this usability/security conflict. Florencio and Herley (2007) and Das et al. (2014) found that password reuse is widespread among web users, with reported reuse affecting approximately 43% to 51% of users (Florencio and Herley, 2007) and (Das et al., 2014). Das et al. (2014) further demonstrated that users frequently modify existing passwords in predictable ways to satisfy different website requirements. Although these modifications may technically produce different passwords, predictable transformation patterns can still be exploited by password-cracking algorithms. Consequently, increasing password complexity requirements may not eliminate insecure behavior and can instead encourage users to adopt predictable strategies for managing multiple credentials (Das et al., 2014).

This relationship between security knowledge and actual behavior is commonly described as the attitude–behavior gap. Herath and Rao (2009) found that employees may hold positive attitudes toward security policies while failing to consistently comply with them because immediate concerns such as convenience, productivity, and time savings can outweigh security considerations (Rao, 2009). Vance, Siponen, and Pahnila (2012) similarly identified the importance of habits and protection motivation in sustaining secure behavior. These findings demonstrate that security awareness alone does not guarantee secure password practices. Users may understand the importance of strong passwords while continuing to reuse credentials or select simpler alternatives when security requirements create excessive inconvenience (Vance, Siponen, and Pahnila, 2012).

Because password security depends on both technical requirements and user acceptance, Information Systems researchers have increasingly applied technology acceptance and behavioral models to understand secure password adoption. Davis's (1989) Technology Acceptance Model (TAM) proposes that perceived usefulness and perceived ease of use influence an individual's intention to adopt and use a technology (Davis, 1989). Building on this theoretical foundation, Novakovic et al. (2009) applied the Unified Theory of Acceptance and Use of Technology (UTAUT) to password security. Their findings indicated that perceptions of effort and performance expectancy influence both users' intentions to employ secure passwords and their actual secure behavior. These findings suggest that password policies imposing excessive cognitive or usability burdens can generate negative attitudes and encourage policy avoidance (Novakovic et al, 2009).

Other research reinforces the importance of user perceptions, self-efficacy, habit, and organizational support. Rhee et al. (2009) identified security self-efficacy as an important factor in security behavior (Rhee et al., 2009), while Bulgurcu et al. (2010) demonstrated the role of security awareness in shaping secure practices (Bulgurcu et al., 2010). Together, these findings indicate that effective password security cannot be evaluated solely by measuring the technical strength of a credential. User perceptions of difficulty, usefulness, confidence, and inconvenience also influence whether secure practices are adopted and maintained.

Human-centered interventions have therefore been proposed to reduce the cognitive burden associated with password security. Passphrases provide one potential solution by allowing users to create memorable credentials while maintaining substantial resistance to guessing attacks (Bonneau et al., 2012). Password managers provide another approach by generating and securely storing credentials, reducing the number of passwords users must remember and potentially reducing password reuse (Das et al., 2014) and (Pearman et al., 2019). However, adoption of these tools is not universal, indicating that technical availability alone does not guarantee behavioral change. Organizational support, appropriate security education, and policies that account for human factors remain important components of effective password security (Herley, 2009).

Overall, the literature demonstrates that password security is not solely a technical problem. While strong passwords and authentication controls provide an important defense against unauthorized access, their effectiveness is constrained by human cognitive limitations and user acceptance. Excessive complexity can encourage insecure coping strategies, while insufficient security requirements can leave organizations vulnerable to credential attacks. The attitude behavior gap further demonstrates that awareness of security risks does not necessarily translate into secure

behavior. Technology acceptance models such as TAM and UTAUT provide a framework for examining how perceived usefulness, ease of use, effort, self-efficacy, and other behavioral factors influence password security practices. Consequently, evaluating password security through both technical and behavioral perspectives provides a more comprehensive understanding of why users comply with, resist, or circumvent organizational password requirements.

3. RESEARCH QUESTION

Prior literature demonstrates that strong, complex passwords significantly enhance information security. However, technical controls are only as effective as end-user compliance. Understanding what drives user adoption of complex password habits is critical for improving overall security posture.

To address this gap, this study uses the Technology Acceptance Model (TAM) as an initial theoretical baseline. Our primary research objectives are to:

- Identify salient adoption factors: Determine the primary perceptual and contextual drivers that lead users to adopt complex password behaviors.
- Evaluate theoretical fit: Assess how effectively core TAM constructs explain password security compliance and habit formation.

4. METHODS

Data were collected using Qualtrics, a cloud-based platform for creating and distributing surveys that also provides built-in data analysis tools (What is Qualtrics?, 2025). The web-based survey was administered from October 24, 2024, through November 7, 2024, and yielded 101 responses. Participants were recruited through Amazon Mechanical Turk (MTurk), an online marketplace that enables individuals and businesses to outsource tasks such as data validation, survey participation, and content moderation (Amazon Mechanical Turk, 2025), as well as through a survey link distributed to students.

Survey questions were derived from questions administered by Donalds and Osei-Bryson (2017) and from the Technology Acceptance Model (TAM) developed by Davis (1989); the complete survey is provided in Appendix A. Because the original TAM construct of Perceived Usefulness (PU) is intended to measure the degree to which an individual believes that a system enhances job or task performance, the corresponding items in this study were adapted to address password security. The modified items focused on participants' perceptions of the effectiveness and value of complex passwords, their confidence in using them, and their behavioral tendencies regarding password security rather than their contribution to productivity or task performance. This study relabeled Perceived Usefulness as Perceived Utility (PU). The revised terminology reflects the broader personal and practical value participants associated with complex passwords. This modification allows the construct to represent participants' perceptions of the security benefits and usefulness of password complexity without implying that complex passwords necessarily improve occupational or task performance. The modified construct therefore maintains the theoretical foundation of TAM while adapting its measurement to the password-security context examined in this study.

This study employs a custom Iterative Independent Variable Selection (IIVS) procedure, illustrated in Figure 1. Variable selection methods are used to systematically identify variables that are most relevant to a particular analytical objective, including regression modeling (Chaurasia & Harel, 2012). Regression-based approaches have also been used to identify dependent and explanatory variables in Information Systems research, including through regression and path-analysis approaches (Richmond et al., 2020) and (Wang et al., 2025).

IIVS is based on the principle of backward elimination, a stepwise variable-selection procedure in which a model initially includes all available independent variables and subsequently removes variables that do not meet a specified statistical significance criterion (Chowdhury & Turin, 2020). In this study, the procedure is applied iteratively across multiple representations of the survey variables rather than being limited to a single regression model. At each iteration, variables that fail to meet the predefined significance threshold are removed, and the resulting model is re-estimated. This process continues until the remaining variables satisfy the selection criterion.

The IIVS procedure is applied at three levels of representation. First, individual survey items are evaluated as independent variables. Second, items are aggregated into averaged construct scores, and the resulting construct-level variables

are evaluated. Third, latent variable scores generated through SmartPLS 4 are subjected to the same variable-selection procedure. Applying the procedure at these multiple levels allows the study to evaluate whether relationships identified at the individual-item level remain present when the variables are represented as construct composites and as latent-variable scores.

The proposed IIVS procedure is intended to complement, rather than replace, established data-reduction and structural-modeling techniques. Its purpose is to identify variables that demonstrate direct predictive relevance to the dependent variable while subsequently examining whether those relationships remain when measurement constructs are modeled using PLS-SEM.

Variable selection is important when adapting theoretical frameworks such as TAM to multi-item survey instruments because individual survey items may contain redundant or overlapping information. Exploratory Factor Analysis (EFA) evaluates the covariance structure among observed variables and groups items according to their underlying relationships. Factor extraction and item retention are therefore based primarily on relationships among the predictors themselves. IIVS instead evaluates candidate variables against the study's target dependent variable, Behavioral Intention to Use (BITU), allowing variables to be retained based on their demonstrated predictive relationship with the outcome rather than solely on inter-item covariance.

IIVS extends the concept of standard backward stepwise regression by applying the elimination procedure across multiple levels of representation. Conventional backward elimination is typically performed using either individual observed variables or composite variables. IIVS applies the procedure sequentially to raw survey indicators, average construct composites, and PLS-SEM latent variable scores. This provides an opportunity to examine whether variable relationships remain consistent as the representation of the underlying constructs changes.

IIVS differs from regularization approaches such as LASSO and Elastic Net in its emphasis on statistical significance and interpretability. Regularized regression introduces penalties that shrink coefficients and can set some coefficients to zero, making it useful for predictive variable selection in high-dimensional datasets. IIVS instead applies an explicit statistical significance threshold of $p < .005$ at each elimination step. This preserves a direct hypothesis-testing framework and allows the retained variables to be interpreted using conventional inferential statistics.

IIVS incorporates a PLS-SEM validation stage using SmartPLS 4. After the measurement model is evaluated, standardized latent variable scores are extracted and used as inputs to a subsequent IIVS procedure. This step examines whether the relationships identified during the observed-variable analysis remain when the constructs are represented as latent variables within a structural equation modeling framework. The approach therefore provides a means of connecting item-level exploratory variable selection with variance-based structural modeling.

Overall, IIVS links iterative backward elimination with multiple levels of variable representation and subsequent PLS-SEM validation. The procedure is designed to reduce redundant variables while maintaining explanatory power, with the study targeting an overall coefficient of determination of $R^2 > .60$. Figure 1 illustrates the sequence of the IIVS procedure, from initial independent-variable selection through construct-level analysis and final validation using SmartPLS 4.

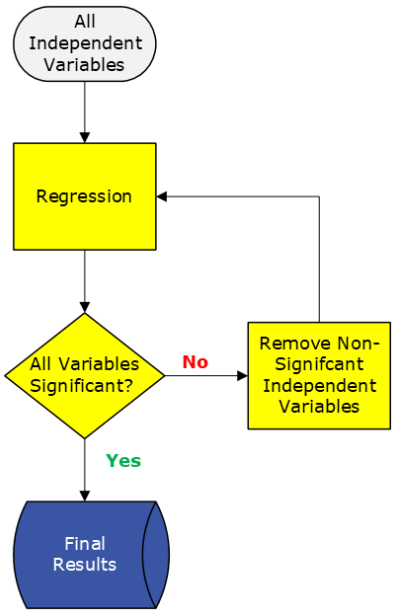


Figure 1: **Iterative Independent Variable Selection**

To further explore predictive relationships, Partial Least Squares Structural Equation Modeling (PLS-SEM) was conducted using SmartPLS 4. Latent

variable scores were generated, and an exploratory model was developed to identify significant predictors of Behavioral Intention to Use (BITU). Non-significant constructs were removed through iterative analyses. The final model retained three key predictors: Attitude Towards Use (AT), General Security Orientation (GSO), and Perceived Utility (PU). All three demonstrated statistically significant relationships with behavioral intention, and the model explained more than 50% of the variance in BITU across the dependent variable configurations examined.

Structural Equation Modeling (SEM) is a multivariate statistical technique that combines factor analysis and multiple regression to estimate interrelated relationships among observable indicator variables and unobservable latent constructs. In Information Systems research, SEM methodologies generally fall into two primary paradigms: Covariance-Based SEM (CB-SEM) and Partial Least Squares SEM (PLS-SEM). CB-SEM focuses primarily on confirming established theoretical models by minimizing the difference between estimated and sample covariance matrices, whereas PLS-SEM is a variance-based, predictive approach that emphasizes the explanation of variance in dependent latent constructs.

PLS-SEM, implemented using SmartPLS 4, was selected as the primary structural modeling method over traditional CB-SEM based on the theoretical and empirical characteristics of this study. First, the study has an exploratory focus, extending the Technology Acceptance Model into the domain of complex password security behaviors while combining structural modeling with the proposed IIVS procedure. PLS-SEM is appropriate for studies that extend theoretical frameworks and seek to identify salient predictors in exploratory research settings. Second, data filtering resulted in a final sample of N = 84 valid responses. PLS-SEM was selected because of its ability to accommodate smaller samples and non-normal data distributions. Third, PLS-SEM generates standardized latent variable scores for each construct, including Perceived Utility, General Security Orientation, and Attitude Towards Use. These scores allow the IIVS procedure to evaluate construct relationships using latent-variable representations rather than unweighted item averages. Finally, because the study focuses on identifying perceptual factors associated with Behavioral Intention to Use complex passwords, PLS-SEM's variance-based estimation approach supports the study's emphasis on explaining variance in BITU.

5. RESULTS

Qualtrics yielded 101 responses. After data cleaning, 12 incomplete responses and five that failed embedded attention-check questions were removed, resulting in 84 valid responses for analysis. To address the seven participants who listed two nationalities in the demographic question (DM3), the variable was split into two fields (DM3_1 and DM3_2). For participants who reported only one nationality, the same value was entered in both fields to maintain consistency.

To ensure consistency in response directionality, 14 survey items were reverse-coded. For instance, item A1_1 was positively worded, while A1_2 was negatively worded; to align their scales, responses to A1_1 were reversed (e.g., a response of 7 was re-coded as 1, 6 as 2, and so on). After reverse-coding, A1_1 and A1_2 responses were within two points of each other for 66 out of 84 participants, indicating consistent interpretation. Similar reverse-coding was applied to items related to Perceived Utility, General Security Orientation, Security Self-Efficacy, and Behavioral Intention to Use, which were either negatively worded or had scales ordered differently from other items. Finally, composite variables were created by averaging responses within each construct to prepare the dataset for regression analysis.

Of these 84 responses, 35 were students. Of these 35, 29 participants were male. Of these 35, the most common age group was 25-34 years old (n=14). White/Caucasian was the most common ethnicity (n=20). 26 described their highest degree of education as High School Diploma. 17 described their employment status as full-time. 33 reported North America as their home, and 22 reported their marital status as single. In summary, this group is mostly high school graduates, single, white, male, 25 – 34 years old, who are full employed and from North America.

Of the 84 responses, 49 responses were acquired using Amazon Mechanical Turk. 32 were male, 21 reported an age range of 35-44 and an additional 21 reported an age range of 45-54. 36 reported as white/Caucasian. 21 reported having completed a bachelor’s degree. 34 were full-time employees, 30 reported North America as the location of their home and 26 reported as being single. In summary, this group is mostly college graduates, single, white, male, 35 - 54 years old, who are full employed and from North America. In comparing the student group to the MTurk group, the student group was in a younger age

group and had less education.

A simple linear regression line follows the equation $Y = a + bX$, where X is the explanatory variable, Y is the dependent variable, a is the intercept (indicating where the line crosses the Y-axis), and b represents the slope, or the expected change in Y for each one-unit increase in X.

Using the 84 valid survey responses, four regression models were developed following the Iterative Independent Variable Selection (IIVS) process. This method involves running a linear regression, removing non-significant variables, and repeating the process until only statistically significant predictors remain. The first three models were conducted using IBM SPSS, while the fourth and final model was developed in SmartPLS 4.

In the first model, mean scores were calculated for each construct, and Behavioral Intention to Use – Averaged (BITUA) was selected as the dependent variable, with all other constructs entered as independent variables (see Table 1). The coefficient of determination (R^2) was used to assess model fit, representing the proportion of variance in the dependent variable explained by the model. In this analysis, a significance threshold of $p < .005$ was applied to determine whether relationships between predictors and the outcome variable were statistically significant (i.e., unlikely to have occurred by chance under the null hypothesis).

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	$.727^a$	.529	.485	.911
a. Predictors: (Constant), SSE, At, PCBI, GCSB, GSA, GSO, PU				

	t	Sig.
(Constant)	.708	.481
AT	-1.310	.194
PU	4.570	<.001
PCBI	2.115	.038
GCSB	.555	.581
GSA	-.562	.576
SEE	-.856	.395

Table 1: **Linear Regression – Averaged Constructs**

The BITUA model yielded an R^2 value of .529. Perceived Utility (PU), General Security Orientation (GSO), and Password Compliance Behavior (PCBI) emerged as significant predictors. Additional regression models were evaluated using BITU2 and then BITU1 as dependent variables. The BITU2 model (excluding BITU1) resulted in an R^2 of .689, with no predictors being statistically significant. The BITU1 model (excluding BITU2) yielded the strongest fit (R^2 = .784), with three items — A2 (Attitude toward Use), PU2_3 (Perceived Utility), and SSE2_2 (Security Self-Efficacy).

In the second regression model, BITU2 was designated as the dependent variable, with all other constructs—excluding BITU1—entered as independent variables (see Table 2). The model produced an R^2 value of 0.689, indicating that approximately 69% of the variance in BITU2 was explained by the predictors. However, only PU1_1 demonstrated statistical significance ($p = .015$), while all other variables failed to reach the significance threshold. Given the limited number of significant predictors, linear regression was considered less suitable for modeling BITU2 as a dependent variable.

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	$.830^a$	.689	.560	.915
a. Predictors: (Constant), SSE2_2, PCB1_1, GSA2_3, PU1_2, GSCB1_2, PCB1_2, GSA1_1, GSCB1_1, PU2_2, A1_1, GSO1_1, SSE2_1, GSA2_1, PU2_3, A2, PU2_1, SSE1_1, SSE1_2, GSO1_2, A2_2, PU1_1, GSA1_2, PU1_3, SSE1_3				

	t	Sig.
(Constant)	.006	.995
A1_1	-1.361	.179
A1_2	.662	.511
A2	.201	.842
PU1_1	2.506	.015
PU1_2	-1.090	.280
PU1_3	1.707	.093
PU2_1	-.219	.827
PU2_2	-.633	.529
PU2_3	1.685	.097
PCB1_1	.163	.871
PCB1_2	1.410	.164
GSCB1_1	-.971	.335
GSCB1_2	-.336	.738
GSA1_1	.020	.984
GSA1_2	.817	.417
GSA2_1	-1.251	.216
GSA2_3	-.267	.791
GSO1_1	1.628	.109
GSO1_2	1.728	.089
SSE1_1	-.972	.335
SSE1_2	-1.101	.276
SSE1_3	.047	.963
SSE2_1	-.331	.742
SSE2_2	1.922	.060

Table 2: **Linear Regression – BITU2 as dependent variable**

A third regression model was run using BITU1 as the dependent variable, excluding BITU2 from the independent variables (see Table 3). This model produced the highest R^2 value (.784), indicating a strong model fit. Among the 24 independent variables, three variables: A2, PU2_3, and SSE2_2, had p-values below .005, identifying them as statistically significant predictors of BITU1. These variables reflect users' comfort with using complex passwords (A2), their frustration with password requirements (PU2_3), and their confidence in learning to protect their information (SSE2_2). To further explore their impact, a final regression model was conducted using only these three predictors (see Table 4), resulting in an R^2 of .626. While this was lower than the full model, it demonstrated that these three factors alone explain a substantial portion of the variance in users' behavioral intention to adopt or continue using complex passwords.

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	886[4]	.784	.695	.722
a. Predictors: (Constant), SSE2_2, PCB1_1, GSA2_3, PU1_2, GSCB1_2, PCB1_2, GSA1_1, GSCB1_1, PU2_2, A1_1, GSO1_1, SSE2_1, GSA2_1, PU2_3, A2, PU2_1, SSE1_1, SSE1_2, GSO1_2, A2_2, PU1_1, GSA1_2, PU1_1, SSE1_3				

	t	Sig.
(Constant)	.342	.734
A1_1	1.458	.150
A1_2	-1.427	.159
A2	5.143	<.001
PU1_1	.735	.465
PU1_2	-1.670	.100
PU1_3	1.121	.267
PU2_1	.540	.591
PU2_2	.024	.981
PU2_3	2.533	.014
PCB1_1	1.253	.215
PCB1_2	.286	.776
GSCB1_1	.191	.849
GSCB1_2	.490	.626
GSA1_1	.176	.861
GSA1_2	.552	.583
GSA2_1	.066	.948
GSA2_3	.029	.977
GSO1_1	-.292	.771
GSO1_2	.513	.610
SSE1_1	.034	.973
SSE1_2	-1.478	.145
SSE1_3	-1.476	.145
SSE2_1	-.676	.502
SSE2_2	2.072	.043

Table 3: **Linear Regression – BITU1 as dependent variable**

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.791[4]	.626	.611	.815
a. Predictors: (Constant), SSE2_2, A2, PU2_3				

	t	Sig.
(Constant)	.953	.343
A2	8.320	<.001
PU2_3	2.133	.036
SSE2_2	-2.34	.815

***Table 4:* Linear Regression – BITU1 as dependent variable and only significant independent variables**

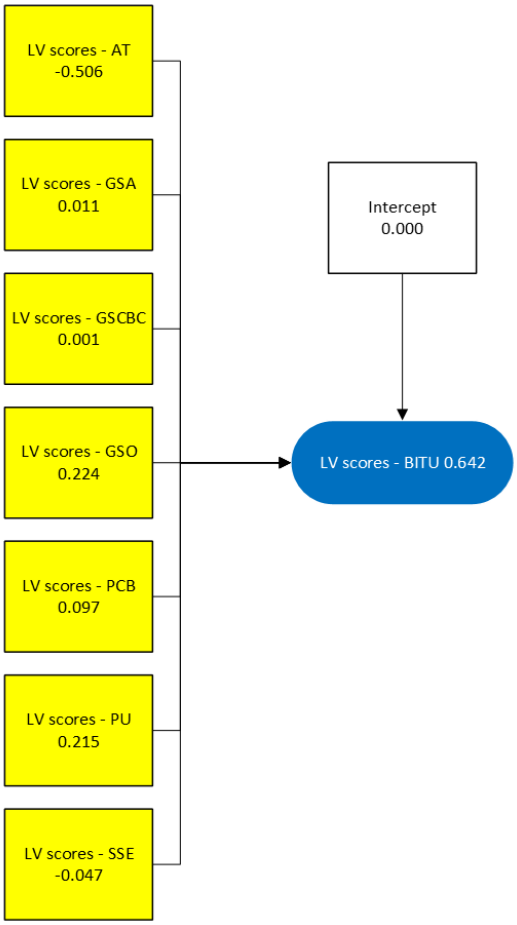


***Figure 2:* Exploratory Regression Model using SmartPLS 4**

To further explore predictive relationships, Partial Least Squares Structural Equation Modeling (PLS-SEM) was conducted using SmartPLS 4 (see Figures 2 and Table 5). Latent variable scores were generated from all survey questions to build an exploratory model predicting Behavioral Intention to Use (BITU). Non-significant constructs were removed through iterative analyses, and the final model retained three statistically significant predictors: Attitude towards Use (AT), General Security Orientation (GSO), and Perceived Utility (PU). These variables explained over 50% of the variance in BITU across multiple dependent variable configurations and were carried forward for subsequent regression modeling.

	T value	**P value**
LV scores - AT	4.555	**0.000**
LV scores - GSA	0.129	0.898
LV scores - GSCBC	0.011	0.991
LV scores - GSO	2.614	**0.011**
LV scores - PCB	1.258	0.212
LV scores - PU	2.03	0.046
LV scores - SSE	0.529	0.598
Intercept	0	1

***Table 5:* Calculated latent variable scores for all questions using SmartPLS4**

6. DISCUSSION

Following an Iterative Independent Variable Selection process, the model with BITU1 as the dependent variable had the highest R^2 value (.784). The significant constructs were A2, PU2_3, and SSE2_2.

A2 (Attitude toward Use) asked participants, "How comfortable are you using complex passwords for your accounts?" The significance of this variable indicates that comfort with complex password use is a critical driver of behavioral intention. Users who feel more at ease using complex passwords are more inclined to continue using them.

PU2_3 (Perceived Utility) measured the item, "Do you find it frustrating to comply with complex password requirements?" It suggests that frustration or lack of perceived value in password complexity negatively impacts users' intentions to adopt secure behaviors.

SSE2_2 (Security Self-Efficacy) was based on the statement, "I feel confident that I can learn methods to protect my information and information system." This item captures users' belief in their own ability to engage in security-

related tasks. Its significance indicates that users with higher self-efficacy. Those who believe they can learn and apply protective measures are more likely to adopt complex passwords. This suggests that confidence in one's ability to manage security plays an important role in motivating protective behaviors in cyber security.

Together, these three variables suggest that behavioral intention to use complex passwords is significantly influenced by users' comfort with the behavior, their perception of its usefulness or ease, and their confidence in managing their own security. For system designers concerned with password policy development, this highlights the need to reduce user frustration, increase perceived value, and build users' confidence through education and intuitive design.

In comparing the dependent variables and their respective significant independent variables, see Table 6, the exploratory regression model using SmartPLS 4 supports the findings of the previous regression models run through IBM SPSS.

Dependent Variable	Significant Independent Variables
BITUA (SPSS)	GSO, PCBI, PU
BITU2 (SPSS)	PU1_1
BITU1 (SPSS)	A2, PU2_3, SSE2_2
BITU (Smart PLS))	AT, GSO, PU

Table 6: **Comparison of dependent variables and their significant independent variables**

After removing the non-significant constructs and rerunning the model in SmartPLS, the results show that Attitude towards Use (AT), General Security Orientation (GSO), and Perceived Utility (PU) are all statistically significant predictors in the regression model. This indicates that each of these factors has a meaningful influence on individuals' intention to adopt strong passwords. As shown in Table 7 and 8 the R^2 values for all endogenous variables exceed 0.60, suggesting that the model explains a substantial proportion of the variance in behavioral intention. This level of explanatory power is comparable to earlier work in the field, such as the Technology Acceptance Model (TAM) by Davis (1989), which similarly identified perceived usefulness as a strong predictor of technology adoption.

	T value	P value
LV scores - AT	5.228	0
LV scores - GSO	2.911	0.005
LV scores - PU	2.177	0.032

Table 7: **Calculated latent variable score for only significant questions using SmartPLS 4**

	LV scores - BITU
R-square	0.633
R-square adjusted	0.619

Table 8: **BITU R^2**

As expected, both General Security Orientation and Perceived Utility had positive effects: individuals who are more security-conscious and who perceive strong passwords as useful are more likely to intend to adopt them. However, Attitude towards Use showed a negative effect, which is unexpected. People who said they felt positive about using strong passwords were less likely to say they planned to use them. This type of gap between what people think and what they do has been seen in other security research. For example, Herath and Rao found that even when employees agreed that security policies were important, they sometimes ignored them because they were inconvenient, time-consuming, or did not fit into their normal work habits (Herath and Rao, 2009). With passwords, people may like the idea of strong passwords in theory but avoid them if they feel they are too hard to remember or take too much effort to create (Vance, Siponen, & Pahnila, 2012). This finding highlights the need for further investigation to better understand how attitude interacts with perceived usefulness and security orientation in shaping password-related behavior.

7. CONCLUSION

This exploratory study gathered data through a Qualtrics survey administered to students and participants recruited via Amazon Mechanical Turk, yielding 84 valid responses after data cleaning. Survey items were adapted from the Technology Acceptance Model (TAM) and from Donalds and Osei-Bryson. Regression and PLS-SEM analyses demonstrated that Attitude towards Use, General Security Orientation, and Perceived Utility significantly predicted behavioral intention to use complex passwords, collectively explaining over 50% of the variance in the final model. Furthermore, we present a method for

independent variable selection designated Iterative Independent Variable Selection (IIVS) and confirmed results via regression with latent variable scores.

These findings align with the broader literature, which underscores the increasing importance and complexity of cyber security. As digital threats grow in scale and sophistication, strong, unique passwords continue to be a frontline defense for both personal and organizational systems. The theoretical foundation provided by TAM helps explain users' adoption of these practices, reinforcing the role of Perceived Utility in fostering stronger password behavior and heightened cyber security awareness.

9. REFERENCES

Adams, A., & Sasse, M. A. (1999). Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures. *Communications of the ACM, 42*(12), 40–46. https://doi.org/10.1145/322796.322806

Amazon. (2025). *Amazon Mechanical Turk*. Retrieved June 4, 2025, from https://www.mturk.com/

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437-443. https://doi.org/10.1016/j.chb.2016.12.040

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes. *2012 IEEE Symposium on Security and Privacy*, 553–567. https://doi.org/10.1109/SP.2012.44

Brown, S. (2010). "Likert Scale Examples for Surveys." from https://www.extension.iastate.edu/documents/anr/likertscaleexamplesforsurveys.pdf.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548. DOI: 10.2307/25750690

Chaurasia, A., & Harel, O. (2012). Using AIC in multiple linear regression framework with multiply imputed data. *Health Services and Outcomes Research Methodology, 12*, 219-233. DOI: 10.1007/s10742-012-0088-8

Chowdhury, M. Z. I., & Turin, T. C. (2020). Variable selection strategies and its importance in clinical prediction modelling. *Family Medicine and Community Health, 8*(1), e000262. DOI: 10.1136/fmch-2019-000262

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, October. DOI: 10.22215/timreview/835

Das, S., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The tangled web of password reuse. *Network and Distributed System Security Symposium (NDSS)*. https://doi.org/10.14722/ndss.2014.23290

Davis, F. D. (1989). *Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology*. Management Information Systems Research Center, 13(Sept): 319-340. https://doi.org/10.2307/249008

Donalds, C., & Osei-Bryson, K.-M. (2017). Exploring the impacts of individual styles on security compliance behavior: A preliminary analysis. *SIG GlobDev 2017 Proceedings, 1*. https://aisel.aisnet.org/globdev2017/1

Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. Proceedings of the 16th International Conference on World Wide Web, (pp. 657–666). ACM. https://doi.org/10.1145/1242572.1242661

Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. *Proceedings of the 2009 New Security Paradigms Workshop*, 133–144. https://doi.org/10.1145/1595676.1595690

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6

John Hopkins University. (2025). What is Qualtrics? John Hopkins University. Retrieved June 4, 2025, from https://uis.jhu.edu/qualtrics/what-is-qualtrics/

Novakovic, L., McGill, T. J., & Dixon, M. W. (2009). Understanding user behavior towards passwords through acceptance and use modelling. International Journal of Information Security and Privacy, 3(1), 11–29. https://doi.org/10.4018/jisp.2009010102

Pearman, S., Thomas, J., Naeini, P. E., Habib, H., Bauer, L., Christin, N., Cranor, L. F., Egelman, S., & Forget, A. (2017). Let's go in for a closer look: Observing passwords in their natural habitat. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 295–310. https://doi.org/10.1145/3133956.3133973

Richmond, H. L., Tome, J., Rochani, H., Fung, I. C.-H., Shah, G. H., & Schwind, J. S. (2020). The use of penalized regression analysis to identify county-level demographic and socioeconomic variables predictive of increased COVID-19 cumulative case rates in the state of Georgia. *International Journal of Environmental Research and Public Health, 17*(21), 8036. doi: 10.3390/ijerph17218036

Rhee, H.-S., et al. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security, 28(8): 816-826. DOI: 10.1016/j.cose.2009.05.008

Special Eurobarometer 390: *Cyber security (v1.00)*. (2014). European Commission, Directorate-General for Communication. https://data.europa.eu/data/datasets/s1058_77_2_ebs390?locale=en

Turan, M. S., Barker, E. B., Burr, W. E., & Chen, L. (2010). *Recommendation for Password-Based Key Derivation––Part 1: Storage Applications* (NIST Special Publication 800-132). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-132

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 27(3), 425-478. https://doi.org/10.2307/30036540

Wang, Z., Li, S., Zhou, X., & Zhu, S. (2025). An iterative conditional variable selection method for constraint-based time series causal discovery. *Chemometrics and Intelligent Laboratory Systems, 260*, 105361. https://doi.org/10.1016/j.chemolab.2025.105361

What is Cybersecurity? (2021, 09/10/2024). https://www.cisa.gov/news-events/news/what-cybersecurity

APPENDIX A

Survey Questions

Construct	Code	Item	Possible Response
Demographics	D1	What gender do you identify as?	Male, Female, I do not wish to specify
Demographics	D2	What is your age?	18-24, 25-34, 35-44, 45-54, 55-64, 65 or older
Demographics	D3	What is your ethnicity?	Hispanic/Latino, Black/African American, White/Caucasian, Native American/American Indian, Asian/Pacific Islander, Other
Demographics	D4	What is your highest degree or level of education you've completed?	High School Degree, Bachelor's Degree, Master's Degree, Doctorate Degree
Demographics	D5	What is your current employment status?	Full-Time, Part-Time, Internship, Retired, Non-employed, Other
Demographics	D6	Where is your home located?	Africa, Asia, Australia, Caribbean/Pacific Island, Europe, North America/Central America, South America, Other
Demographics	D7	What is your marital status?	Single, Married, Divorced, Widowed
Perceived Utility of Complex Passwords	PU1_1	Do you feel that using complex passwords improves the security of your personal information? (Davis, 1989)	7-point Likert Scale for Agreement (Brown, 2010)
Perceived Utility of Complex Passwords	PU1_2	How confident are you that complex passwords protect sensitive data? (Davis, 1989)	7-point Likert Scale for Agreement (Brown, 2010)
Perceived Utility of Complex Passwords	PU1_3	To what extent do you believe complex passwords are necessary for protecting your accounts from cyber threats? (Davis, 1989)	7-point Likert Scale for Agreement (Brown, 2010)
Perceived Utility of Complex Passwords	PU2_1	Do you think using complex passwords helps prevent unauthorized access to your accounts? (Davis, 1989)	7-point Likert Scale for Agreement (Brown, 2010)
Perceived Utility of Complex Passwords	PU2_2	How easy is it for you to create and remember complex passwords? (Davis, 1989)	7-point Likert Scale for Agreement (Brown, 2010)
Perceived Utility of Complex Passwords	PU2_3	Do you find it frustrating to comply with complex password requirements? (Davis, 1989)	7-point Likert Scale for Agreement (Brown, 2010)

Attitude Toward Use	A2	How comfortable are you using complex passwords for your accounts? (Venkatesh et al., 2003)	6-point Likert scale for Likelihood (Brown, 2010)
Attitude Toward Use	A1_1	Would you prefer simpler password policies even if they meant less security? (Venkatesh et al., 2003)	7-point Likert Scale for Agreement (Brown, 2010)
Attitude Toward Use	A1-2	Do you feel more secure when using complex passwords? (Venkatesh et al., 2003)	7-point Likert Scale for Agreement (Brown, 2010)
Behavioral Intention to Use	BITU1	How likely are you to adopt or continue using complex passwords for your accounts in the future? (Venkatesh et al., 2003)	6-point Likert scale for Likelihood (Brown, 2010)
Behavioral Intention to Use	BITU2	Would you recommend using complex passwords to others? (Venkatesh et al., 2003)	7-point Likert Scale for Agreement (Brown, 2010)
Password Compliance Behavior	PCB1_1	I use unique passwords for each account. (e.g. online banking, social media, email) (Anwar et al., 2017) (Donalds & Osei-Bryson, 2017) (Special Eurobarometer 390: Cyber security (v1.00), 2014)	6-point Likert scale for Likelihood (Brown, 2010)
Password Compliance Behavior	PCB1_2	I have changed my passwords in the past 12 months. (Anwar et al., 2017) (Donalds & Osei-Bryson, 2017) (*Special Eurobarometer 390: Cyber security (v1.00)*, 2014)	6-point Likert scale for Likelihood (Brown, 2010)
General Security Compliance Behavior	GSCB1_1	I never send sensitive information in plaintext via email or social media (e.g. bank account numbers, pins, passwords) (Anwar et al., 2017) (Donalds & Osei-Bryson, 2017) (*Special Eurobarometer 390: Cyber security (v1.00)*, 2014)	6-point Likert scale for Likelihood (Brown, 2010)
General Security Compliance Behavior	GSCB2_2	I only visit websites that I know or trust. I only click on URL links if I know where the URL will take me. (Anwar et al., 2017) (Donalds & Osei-Bryson, 2017) (*Special Eurobarometer 390: Cyber security (v1.00)*, 2014)	6-point Likert scale for Likelihood (Brown, 2010)
General Security Awareness	GSA1_1	I understand the concerns of cyber security threats and the risks that they pose. (Bulgurcu et al., 2010) (Donalds & Osei-Bryson, 2017)	6-point Likert scale for Likelihood (Brown, 2010)
General Security Awareness	GSA1_2	I am aware of potential information/cyber security threats and their negative consequences. i.e. I know about different types of cyber security threats such as phishing emails, social engineering, and/or denial of service attacks, etc. (Bulgurcu et al., 2010)	6-point Likert scale for Likelihood (Brown, 2010)

		(Donalds & Osei-Bryson, 2017)	
General Security Awareness	GSA2_1	I have sufficient knowledge of the costs of cyber security threats. (Bulgurcu et al., 2010) (Donalds & Osei-Bryson, 2017)	6-point Likert scale for Likelihood (Brown, 2010)
General Security Awareness	GSA2_3	I read cyber security bulletins or newsletters. (Donalds and Osei-Bryson 2017)	6-point Likert scale for Likelihood (Brown, 2010)
General Security Orientation	GSO1_1	Cyber security incidents concern me, and I try to take action to prevent them. (Donalds and Osei-Bryson 2017)	7-point Likert Scale for Agreement (Brown, 2010)
General Security Orientation	GSO1_2	I am mindful about computer security. (Donalds and Osei-Bryson 2017)	7-point Likert Scale for Agreement (Brown, 2010)
Security Self-Efficacy	SSE1_1	I feel confident that I can update operating systems using security patches. (Donalds & Osei-Bryson, 2017) (Anwar et al., 2017) (Rhee et al., 2009)	7-point Likert Scale for Agreement (Brown, 2010)
Security Self-Efficacy	SSE1_2	I feel confident that I can set a web browser security level. sei-Bryson, 2017)	7-point Likert Scale for Agreement (Brown, 2010)
Security Self-Efficacy	SSE1_3	I feel confident that I can use different programs to protect my information and information system. (Donalds & Osei-Bryson, 2017) (Anwar et al., 2017) (Rhee et al., 2009)	7-point Likert Scale for Agreement (Brown, 2010)
Security Self-Efficacy	SSE1_4	I feel confident in handling virus infected files and ridding my system of malware. (Donalds & Osei-Bryson, 2017) (Anwar et al., 2017) (Rhee et al., 2009)	7-point Likert Scale for Agreement (Brown, 2010)
Security Self-Efficacy	SSE1_5	I feel confident that I can learn methods to protect my information and information system. (Donalds & Osei-Bryson, 2017) (Anwar et al., 2017) (Rhee et al., 2009)	7-point Likert Scale for Agreement (Brown, 2010)

Beyond Awareness: Building Digital Resilience Through Comprehensive Cybersecurity Foundations for K-5 Students

Ellie Ebrahimi
ebrahimie@uncw.edu

Yasin Emre Gokce
gokcey@uncw.edu

Marjorie Pare
parem@uncw.edu

Berker Koyuncu
bk9560@uncw.edu

Jude Vargas
jrv4914@uncw.edu

Jacob Blount
jmb7970@uncw.edu

Congdon School of Business
University of North Carolina Wilmington
Wilmington, NC 28403, USA

Abstract

This paper introduces Cybersecurity Practice and Awareness for Rising Kids (Cyber-PARK), an innovative cybersecurity education platform specifically designed for K–5 students. Cyber-PARK aims to empower teachers and parents by offering a comprehensive suite of interactive tools, including PowerPoint presentations, videos, worksheets, hands-on activities, and video games. These resources are designed to facilitate the seamless integration of digital safety lessons that align with state and federal guidelines. The platform fosters early digital literacy and builds resilience against online threats, preparing the next generation for a secure digital future. This paper will detail the Cyber-PARK curriculum, outlining its modules and lessons. Furthermore, it will present empirical evaluations from usability testing conducted with diverse groups, including K-5 students, high school students, K-5 STEM/Technology/Media teachers, and cybersecurity experts. The results of these experiments highlight the engagement and comprehension of the content by students, the usability and adaptability of the materials for teachers, and the expert validation of the curriculum's relevance and importance. The insights gained from these evaluations have been instrumental in refining the Cyber-PARK platform, ensuring its scientific soundness and practical effectiveness in addressing the critical need for early cybersecurity education.

Keywords: Cybersecurity, K-5 Education, Gamified Learning, Digital Literacy, Teacher Training, Usability Testing

Recommended Citation: Ebrahimi, E.E., Gokce, Y., Pare, M., Koyuncu, B., Vargas, J., Blount, J., (2026). Beyond Awareness: Building Digital Resilience Through Comprehensive Cybersecurity Foundations for K-5 Students. *Cybersecurity Pedagogy and Practice Journal;* v5(n2) pp 132-147. DOI# https://doi.org/10.62273/SZNX5114

Beyond Awareness: Building Digital Resilience Through Comprehensive Cybersecurity Foundations for K-5 Students

Ellie Ebrahimi, Yasin Emre Gokce, Marjorie Pare, Berker Koyuncu, Jude Vargas, and Jacob Blount

1. INTRODUCTION

In an increasingly digital world, equipping young children with foundational cybersecurity knowledge and digital literacy skills is essential. Just as children learn to safely navigate physical environments, they must also learn to navigate the online world securely. The widespread engagement of K-5 students with online platforms, social media, and gaming exposes them to various risks, including cyberbullying, online predators, privacy breaches, and scams. Despite this heightened digital immersion, there remains a critical lack of foundational cybersecurity education for this age group, leading to a dangerous knowledge gap.

Cybersecurity Practice & Awareness for Rising Kids (Cyber-PARK) addresses this urgent need by providing a browser-based, gamified learning platform designed to instill essential cybersecurity knowledge and digital literacy in K-5 students. This initiative is crucial not only for protecting children from immediate online dangers but also for cultivating critical thinking skills, fostering responsible online behavior, and building an early pipeline for the rapidly growing cybersecurity workforce, thereby mitigating a significant national shortage (Furnell, 2021). Additionally, early exposure to cybersecurity concepts can spark interest in STEM fields, opening doors to future technical careers and developing valuable problem-solving and analytical skills.

The Cyber-PARK education kit is designed with North Carolina Computer Science standards, NC Digital Learning Plan Initiatives, and industry certifications in mind. It aims to streamline the educational experience for teachers and parents by offering a single, comprehensive resource that includes classroom course material, interactive games, and a website for monitoring student progress. The curriculum covers vital topics such as data privacy, internet safety, and digital footprints, with each module aligning with NC K-12 computer Science standards (See Appendix A). The accompanying website serves as a knowledge hub, allowing parents and teachers to track student progress through carefully designed modules.

The current landscape of cybersecurity education for elementary schools faces several challenges:

- **Curriculum Priorities:** Schools often prioritize core subjects, viewing cybersecurity as secondary rather than essential.
- **Lack of Teacher Training:** Many educators lack the necessary cybersecurity knowledge or training, hindering effective instruction.
- **Limited Resources & Funding:** Budget constraints can prevent schools from investing in cybersecurity programs, software, or professional development.
- **Lack of Standardization:** Unlike established subjects, cybersecurity education lacks a widely accepted, standardized curriculum, leading to inconsistencies across schools.
- **Rapidly Evolving Threats:** The dynamic nature of cyber threats makes it challenging for educational materials to remain current.
- **Parental & Administrative Awareness:** A lack of full understanding regarding the importance of early cybersecurity education can lead to insufficient demand and support.

By equipping students with crucial online safety skills, Cyber-PARK helps bridge the digital divide, granting young students and their families greater access to valuable online resources and future employment opportunities. This initiative delivers significant societal benefits by reducing vulnerability to cyber threats while fostering digital inclusion. This paper will elaborate on the Cyber-PARK curriculum and present the empirical findings from usability testing conducted with students, teachers, and cybersecurity experts, providing insights into the effectiveness and relevance of the current approach.

2. LITERATURE REVIEW

Improving STEM (Science, Technology, Engineering, and Mathematics) skills is a current and future imperative for addressing the complex social and economic challenges society faces (Onoshakpokaiye and Avwiri, 2025). STEM education is not merely about preparing students for specific technical careers; it is fundamentally about cultivating essential problem-solving, analytical, and critical thinking skills that are vital

for success across all career paths and in daily life (National Science Teaching Association, 2020). The urgency of this goal is highlighted by existing and projected shortages in the STEM workforce (Kodey et al., 2023; Zaza et al., 2020; Furnell, 2021). The Committee on STEM Education of the National Science and Technology Council emphasizes that STEM competencies are crucial for overall life success, extending far beyond traditional STEM professions (Maclsaac, 2019).

A highly effective pedagogical approach for fostering these critical skills is Problem-Based Learning (PBL). Grounded in situated cognition theory, which posits that "knowing is doing" and that knowledge application is intrinsically linked to its context (Anggraeni et al., 2023; Acton, 2023), PBL requires students to engage with realistic problems. This methodology empowers students to take control of their learning, utilizing teachers as inquiry coaches while working collaboratively. PBL has consistently yielded positive outcomes for students in areas such as collaboration (Mumtahana et al., 2026), student engagement (Nemakhavhani, 2024), and crucially, the development of critical thinking and problem-solving skills (Xu et al., 2023). Research indicates that PBL can significantly increase long-term knowledge retention and improve both test scores and overall problem-solving abilities. Furthermore, PBL offers valuable learning scaffolds that enrich inquiry and enhance student engagement, making it an ideal framework for developing the foundational cognitive skills necessary for navigating complex fields like cybersecurity.

The Imperative of Early Cybersecurity Education

The importance of K-12 cybersecurity education cannot be overstated in today's digitally driven world. Children are increasingly engaged in online activities through school, social media, and gaming platforms, often from a very young age (Anderson and Juang, 2018). This pervasive digital immersion, while offering numerous benefits, also exposes them to a growing array of potential threats, including phishing scams, online predators, and privacy breaches. Cybersecurity education is therefore crucial for helping them identify and avoid these dangers (Quayyum et al., 2021). Teaching children to protect their personal information, such as names, addresses, and locations, is vital for preventing identity theft and reducing the risks of cyberbullying. Moreover, cybersecurity education fosters digital literacy, enabling children to comprehend the broader digital environment, including ethical technology use and the ramifications of their online actions.

Despite this critical need, there remains a noticeable scarcity of cybersecurity curricula specifically designed for students in grades K-5, largely due to perceptions about their developing computer skills and knowledge (Xu and Li, 2025). However, early childhood is widely considered an optimal time for learning, suggesting that introducing cybersecurity or digital literacy in elementary schools could create significantly greater opportunities for future careers and safer digital habits. It is imperative to offer early exposure to cybersecurity principles to protect young children from "negative experiences" (Giannakas et al., 2019; National Science Foundation, 2020; Xu and Li, 2025). Such early curricula can enhance student awareness of cyberattack dangers while proactively introducing them to cybersecurity-related topics before they encounter more complex threats.

Focusing on the grades K-5 demographic also allows researchers to mitigate developmental, behavioral, and technology-access issues often associated with older students. This early intervention provides a crucial opportunity to longitudinally assess the long-term impact of training on students' perceptions of cybersecurity as they reach middle school and beyond. Research indicates that students in middle and high school grades often begin to perceive their academic ability as a "fixed quality," which can lead them to withdraw from subjects where they lack confidence (Jethwani et al., 2016) or a sense of belonging (Jethwani et al., 2017). Introducing cybersecurity concepts at an earlier, more malleable stage can prevent these issues, fostering a positive disposition towards the field.

Designing Effective Curricula: Embracing Diverse Learning Styles and Methodologies

Effective teaching and learning are inherently intertwined, with learning occurring most naturally when instruction is optimal and aligns with the diverse learning styles of the learners (Felder, 2020; Cabual, 2021). Educators teaching the "virtual generation," who are native to digital environments, must leverage new technologies, such as internet-based tools and games, to increase participation and achieve learning objectives (Höfrová et al., 2024; Szymkowiak et al., 2021). Research has consistently demonstrated that virtual technologies can significantly enhance student performance (Han, 2020).

Consequently, game-based technology and strategies have gained substantial momentum in educational settings and have been shown to increase knowledge retention (Putz et al., 2020; Ortiz-Rojas et al., 2019; Kim et al., 2017). With game-based technologies, students can visualize abstract concepts and perform hands-on tasks, moving beyond mere imagination (Parthasarathy et al., 2023; Mikrouli et al., 2024). A growing body of research suggests that when students interact with and control events using emerging technologies, they become more actively involved in constructing knowledge through immersive experiences, as opposed to passive learning methods like lectures or reading (Pflieger et al., 2024). This active engagement is particularly vital for complex and abstract topics like cybersecurity, where practical application and experiential learning can solidify understanding.

Moreover, disparities in science education, particularly in rural, low-income areas, can exacerbate student engagement issues, especially for those with diverse learning needs. Traditional textbook-lecture formats often involve substantial independent analysis of expository writing and worksheet activities, which can be challenging for students rapidly introduced to new theories, facts, and vocabulary in an inconsistent manner. Many general education teachers also lack adequate training or experience in accommodating students with special needs. The proper integration of diverse technologies and pedagogical approaches, such as game-based learning and problem-based learning, into the curriculum has been shown to effectively overcome some of these obstacles, making education more accessible and engaging for all students.

Cybersecurity Education as a Pathway to Future Workforce Development

Cybersecurity workforce development is not merely an academic concern but a critical national and global need for addressing pressing societal, social, and economic challenges. Improving STEM skills is a current and future imperative (Onoshakpokaiye and Avwiri, 2025), and the urgency of this goal is highlighted by existing and projected shortages in the STEM workforce (Kodey et al., 2023, Zaza et al., 2020). The cybersecurity sector, in particular, faces a severe talent gap, with hundreds of thousands of open positions globally (ISC2 Cybersecurity Workforce Study, 2023). This shortage poses significant risks to national security, economic stability, and individual privacy.

The Committee on STEM Education of the National Science and Technology Council emphasizes that STEM skills are vital not only for specialized STEM careers but for all career paths, as they contribute to overall life success (MacIsaac, 2019). Therefore, early exposure to cybersecurity education serves a dual purpose: it protects young individuals in their digital lives today and simultaneously cultivates the foundational knowledge and interest necessary to build the cybersecurity workforce of tomorrow. By introducing cybersecurity concepts at the elementary level, we can spark curiosity, demystify the field, and encourage a diverse range of students to consider careers in this critical domain. This proactive approach to education is essential for creating a robust pipeline of skilled professionals, addressing the current workforce deficit, and ensuring a more secure digital future for all.

3. CURRENT CYBERSECURITY EDUCATION SOLUTIONS

The critical need for early cybersecurity education for K-5 students is underscored by their increasing digital engagement and the prevalent online threats they face. Despite this growing exposure, current educational approaches largely fall into two categories: passive learning (e.g., videos, lectures) and active/gamified learning. While passive methods efficiently deliver foundational knowledge, they often lack the interactivity crucial for sustained engagement and deep comprehension in young learners. For instance, platforms like Tynker offer cybersecurity curriculum through videos and quizzes, but these often lack the interactive experiences necessary to solidify understanding. Similarly, Trend Micro Cyber Academy and MalwareBytes provide information-rich videos, yet they frequently lack interaction, may lose viewer attention, and crucially, do not provide opportunities for assessing knowledge retention without supplemental materials.

Existing active learning resources, though generally more engaging, often prove too complex or text-heavy for elementary students, or they do not offer comprehensive, measurable learning outcomes. For example, the PBS NOVA Labs - Cybersecurity Lab game, while interactive, requires a lengthy tutorial and extensive reading, which can deter younger users. Cyber Sprinters also teaches through interactive elements but relies heavily on text and does not allow for active practice of real-world techniques. Even resources from the Center for Development of Security Excellence, which include word searches, are

often geared towards an adult audience and can be overly text dependent. Furthermore, a common deficiency across many existing activities is the absence of formal knowledge assessment, leaving educators and parents without clear indicators of a child's understanding and ability to apply the material. This collective absence of age-appropriate, truly interactive content, combined with a lack of measurable learning outcomes, highlights a significant and critical gap in effectively designed cybersecurity education activities for young audiences.

The Cyber-PARK project directly addresses these limitations. By developing a curriculum that integrates hands-on activities with gamified learning experiences (e.g., Password Chef, Two-Step Treasures, Potion Post), Cyber-PARK provides simplified, experiential learning opportunities. The Cyber-Park methodology prioritizes active participation and immediate feedback to enhance engagement and comprehension. Furthermore, the inclusion of built-in assessment mechanisms within the games and activities provides clear indicators of student understanding, a crucial feature often missing in current offerings. This approach ensures that Cyber-PARK not only introduces essential cybersecurity principles but also fosters digital resilience through practical application and measurable learning outcomes, effectively bridging the identified gaps in early cybersecurity education.

4. THE CYBER-PARK CURRICULUM

The Cyber-PARK curriculum is designed to provide K-5 students with essential cybersecurity knowledge and digital literacy through a structured, standards-aligned learning journey. It is built around four comprehensive modules, each comprising four dynamic lessons. These modules are equipped with clear objectives, relevant vocabulary, and hands-on materials included in the starter kits, providing educators with everything they need to deliver engaging instruction. Educators set up their classrooms by grade level, which automatically populates age-appropriate content. Although the core lessons are often consistent across all age groups, they are differentiated by adjusting the content's complexity, activities, and assessment methods. The lessons are designed to last at most 30 minutes for one lesson per week.

Here is a detailed breakdown of the Cyber-PARK modules and their respective lessons:

- *Module 1: Digital Foundations*
  - Devices: Students learn to understand basic digital elements.
  - Network & Internet: Introduces how various digital components connect.
  - Accounts & Passwords: Covers fundamental security concepts related to accounts and passwords.
  - Digital Footprints: Explores what information we leave behind online.

- *Module 2: Online Protections*
  - Password Building: Teaches strategies for creating strong, memorable passwords.
  - Social Etiquette: Focuses on positive online interactions.
  - Malicious Actors: Helps students understand who poses threats online.
  - Password Cracking (Basics): Demonstrates how weak passwords are vulnerable.

- *Module 3: Threat Identification*
  - Multi-Factor Authentication (MFA): Explains how to add layers of security to accounts.
  - Phishing: Teaches students to identify online scams.
  - Catching Misinformation: Focuses on critical evaluation of online content.
  - Cyberbullying: Covers identifying and reporting cyberbullying.

- *Module 4: Future & Responsibility*
  - How Technology Evolves: An introduction to concepts like Deepfakes & AI.
  - Careers in Cybersecurity: Explores pathways for future professionals in the cybersecurity field.
  - Safety in Numbers & Responsible Digital Citizenship: Emphasizes responsible online behavior.
  - Maintaining Digital Habits: Focuses on lifelong online safety practices.

Figure 1: Starter kit for in-class activities. The sharpie shows the relative size of the objects in the kit.

Each module utilizes a specially designed starter kit to empower teachers with tangible tools. These kits include (Figure 1):

- 3D Printed Items: Physical models, such as device components, for tactile engagement.
- Multi-Purpose Cards: Versatile cards for activities like password creation, network simulations, and scenario role-playing.

Current Games in Cyber-PARK

The browser-based game platform, Cyber-PARK, is actively under development to provide K-5 students with essential cybersecurity knowledge, skills, and abilities through engaging, age-appropriate activities. It currently includes several proof-of-concept games covering topics such as two-factor authentication (2FA), strong password creation, social engineering, phishing, encryption, and malware injections. The platform is designed to be an engaging and immersive learning environment, allowing for the collection and storage of relevant data to track student progress and performance. The games are integrated into a large, interactive map where each section represents a unique themed area. Students navigate this map as caretakers or explorers, engaging with diverse challenges and objectives. Completing modules unlocks virtual rewards such as pets, tools, or resources specific to the map area. The modules combine problem-solving, critical thinking, and subject-specific skills, and students can personalize their rewards and map areas. Collaboration can also be incorporated to unlock special regions or solve larger challenges.

Currently, three games, Password Chef, Two-Step Treasures, and Potion Post, have been functionally tested by adult and student volunteers, and their design and performance are continuously being refined. The knowledge assessment components have been refined to measure the effectiveness of these games in conveying cybersecurity concepts.

Password Chef: Password Chef is a 2D point-and-click game designed to teach players about creating secure passwords by likening the process to cooking in a restaurant (Figure 2). Players create and memorize unique "dishes" (passwords) by combining virtual ingredients: vegetables (uppercase/lowercase letters), meats (numbers), and spices (special characters). The game requires players to meet specific criteria for password complexity and rewards them based on the strength of their creations. In later stages, players must recall previously created "dishes" for repeat customers, reinforcing memory and retention of strong password practices. This game assesses password growth and recalls over time. The game provides simple touch controls, making it accessible even for players unfamiliar with games. The narrative encourages players to create memorable and secret "recipes" to prevent other "chefs" from guessing them. Challenges progressively increase in complexity, requiring specific character types or minimum lengths. The

Figure 2: Password Chef is a 2D point-and-click game that encourages learners to develop their password safety skills through cooking.

focus is on rewarding successes, empowering players. Password Chef is built using Unity Game Engine and can be deployed as a WebGL or desktop application (See Appendix A – Modules 1 and 2).

Two-Step Treasures: Two-Step Treasures is a 2D point-and-click game that introduces players to the concept of multi-factor authentication (MFA) (Figure 3). Initially, players learn about single authentication factors by creating simple image-based passwords related to personal preferences (e.g., favorite color, animal, or shape). Jigsaw pieces representing these factors are used to unlock treasure chests. After each successful attempt, tooltips provide information about authentication methods, preparing players for subsequent sections. Quiz questions about authentication factors are administered at the end of each stage to assess understanding.

As players advance, they are introduced to various authentication methods, including fingerprint scanners, one-time passwords, and facial recognition technology. Unlocking treasure chests then requires multiple jigsaw pieces, combining knowledge factors with possession or inheritance factors. For instance, players might use a fingerprint to unlock a device to retrieve a second key or use facial recognition for identity verification. The game progressively increases

the complexity of authentication methods and quiz questions. Player assessment is based on quiz results and stage completion. This game is built using the Unity Game Engine, which aims to introduce 2FA in an easy-to-understand format, without time restrictions or consequences for incorrect guesses, allowing for experimentation and understanding of its protective benefits (See Appendix A – Module 3).

Figure 3: Learners will practice one-step authentication, and then, they will be introduced to two-step authentication.

Potion Post: Potion Post is a 2D educational game focused on teaching players to identify common internet scams, such as prize scams, phishing scams, and pyramid schemes (Figure 4). The game presents text-based interactions within the context of a small shop. Players respond to messages by stamping them green for legitimate or red for scams, while also providing requested items or information. Correctly identifying scams rewards players with virtual currency, while incorrect decisions result in currency losses or loss of items, reinforcing the consequences of falling for scams. The game is broken into three stages, each introducing a new type of scam with progressively harder goals and more messages. Data collected includes click locations, time per stage, time per message, total game time, game score, game goal, and the proportion of messages correctly or incorrectly identified. This data is communicated to the server via HTTPS request. Built in Godot Engine, it can be deployed as a WebGL or desktop application. This design allows players to be entertained and challenged while developing their understanding of scam awareness, connecting their in-game actions to real-world impacts (See Appendix A – Module 3).

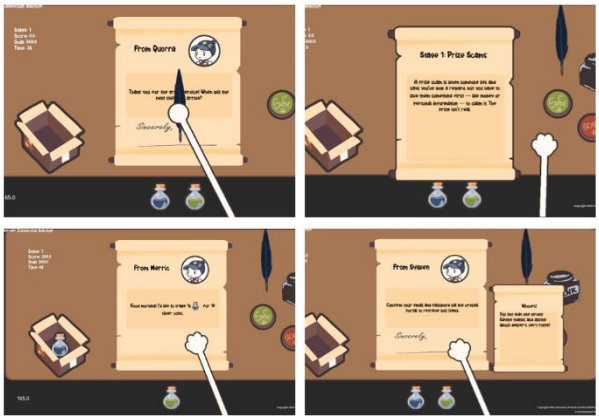


Figure 4: Potion Post allows players to practice identifying scams as potion merchants.

5. METHODOLOGY

To ensure the effectiveness and age appropriateness of the Cyber-PARK curriculum and its interactive components, three sets of usability testing and consultations with distinct target audiences and expert groups have been conducted. This empirical evaluation provided rich qualitative data to refine the materials. This study has been approved by the Institutional Review Board (IRB #03072025) of the University of North Carolina Wilmington and conducted in the summer of 2025. The evaluation involved the following groups:

- Students:
  - Two summer camp groups (25 and 31 students, ages 8-11).
  - 18 individual K-5 students from various grade levels.
  - 5 high school students (to gather general feedback on content and identify areas for additional K-5 content).
- Teachers:
  - 15 K-5 STEM/Technology/Media teachers.
- Cybersecurity Experts:
  - Over 20 experts, including university professors, researchers, and industry/IT security professionals.

Question	Pre-test Responses (N=20)	Post-test Responses (N=16)	Key Improvement
Q1: Familiarity	60% "No/IDK"	62.5% "Yes"	Significant increase in familiarity with the terms.
Q2: Two-Step Purpose	Vague, "extra safety"	More detailed, "harder for hackers", "proves it's you"	Better understanding of the mechanism of security.
Q3: Fingerprint vs. Password	Highlighted "uniqueness"	Repeated the same point, more confidently, and added that passwords can be "copied" or "repeated"	Reinforced understanding of why biometrics are more secure.
Q4: Examples of Factors	Limited examples (phone number, face ID)	Expanded examples across multiple factor types (know, have, are)	Broader and more comprehensive knowledge of security methods.

Table 1: Student improvement analysis on multifactor authentication

Participant Recruitment and Study Context: Usability evaluations were conducted across two separate week-long cohorts of the Seahawk Summer Camp in June of 2025. Camp participants (Cohort 1: n=25; Cohort 2: n=31; ages 8–11) were recruited via open registration through university youth outreach programs, offered free of charge to eliminate socioeconomic barriers. Within each cohort, the Cyber-PARK curriculum was deployed as an intensive single-day instructional module. A subset of participants (n=20 pre-test, n=16 post-test) completed the formal multi-factor authentication assessment module, with minor attrition resulting from early dismissals and incomplete paper surveys. Supplementary individual K–5 learners (n=18) and high school testers (n=5) were recruited through convenience sampling of local school contacts to evaluate module pacing, reading levels, and interface ergonomics.

The testing protocol varied slightly for each group to best gather relevant feedback:

Student Testing: Paper-based pre-assessments were administered immediately prior to module instruction to establish baseline knowledge. During instructional delivery, researchers utilized structured observation sheets to record real-time student engagement, points of confusion, and peer collaboration during physical kit activities. Post-assessments were completed immediately following the hands-on and digital gameplay sessions. Digital telemetry data from game modules (e.g., attempt counts, completion time, password complexity scores, and message classification accuracy) were logged via automated requests. K-5 and high school students provided direct feedback on the age-appropriateness and relevance of the content.

Teacher Testing: Teacher feedback was gathered through semi-structured, 45-minute focus group discussions following hands-on kit walkthroughs, accompanied by an open-ended feedback form evaluating pedagogical alignment and grade-level differentiation. Their feedback was crucial for identifying practical usability issues.

Cybersecurity Expert: Expert evaluations were collected via structured review rubrics and written feedback covering factual correctness, threat taxonomy accuracy, and alignment with national workforce frameworks.

6. RESULTS

Quantitative assessment data (pre- vs. post-intervention item scores and game telemetry metrics) were evaluated using descriptive and comparative statistics to determine knowledge gains and procedural accuracy across cohorts. Qualitative data, comprising written teacher responses, observational notes, and expert commentary, underwent inductive thematic analysis. Two independent researchers coded qualitative feedback into operational categories (e.g., Vocabulary Accessibility, Instructional Scaffolding, Technical Usability, and Curricular Alignment), resolving discrepancies through consensus review to guide iterative revisions.

Content and Construct Validity: Curricular content and assessment questions were constructed in direct alignment with North Carolina K–12 Computer Science Standards and ISTE guidelines. Content validity was established through formal panel review by over 20 academic and industry cybersecurity experts who verified

the technical accuracy and age-appropriateness of the core concepts.

Feasibility: Iterative review rounds with 15 active K–5 STEM, media, and technology educators ensured high face validity, confirming that instructional tasks, reading levels, and visual representations accurately reflected elementary classroom capabilities.

Measurement Reliability: Standardized, scripted lesson plans, uniform visual starter kits, and structured assessment prompts were used across all testing cohorts to minimize delivery variance and ensure administrative reliability across sessions.

Quantitative and Qualitative Data

Student Feedback: The two summer camps (grades 4 and 5) provided invaluable data on the lessons provided and step-by-step activities. Students were highly engaged during the PowerPoint presentations, actively participating in discussions and responding well to prompt questions. Their curiosity and engagement were evident through the insightful talking points and questions they raised. For the hands-on activities, students demonstrated significant enthusiasm, moving around and actively participating, a stark contrast to passively listening to instructions. They explicitly stated that "doing it" helped them understand the concepts better, indicating a strong preference for active learning. Pre- and post-assessments consistently showed improved comprehension of the concepts after the combination of PowerPoint presentations and group activities. The overall level of engagement was significantly higher during the interactive group activities (see table 1). For example, the data from the lesson on MFA suggests an overall improvement in the students' understanding of multifactor authentication, particularly in their ability to define and provide examples of different authentication factors. In the pre-test, many students were unfamiliar with terms like "two-step verification" or "multi-factor authentication," with 12 out of 20 saying they had never heard of them. However, in the post-test, a majority of students (10 out of 16) responded "yes" when asked if they knew the terms. This indicates a significant increase in their familiarity. Students also demonstrated a better grasp of the purpose and mechanics of these security measures. In the pre-test, responses to why two-step verification is used were often vague, mentioning general concepts like "extra security" or to ensure it's "the right person". By the post-test, their answers were more specific, explaining that it makes it harder for hackers to get in because they would need "two passwords" or the code from a "connected device". Furthermore, their ability to name different types of security factors expanded. Initially, examples were limited to passwords, phone numbers, and codes. In the later test, students provided a wider range of examples, including facial recognition, fingerprints, PIN numbers, and email, showing they now understood a broader spectrum of authentication methods (See table 1 for more information).

All students in the K-5 group tested the Password Chef game, and their passwords became significantly longer and stronger with a variety of characters after only three attempts. In the next stage of the game, students will practice techniques to remember their passwords. Two-Step Treasure helped students to learn what the three factors are and identify them correctly after interacting with the game for an average of 30 minutes. Potion Post game has only been tested for its usability and game mechanics.

Teacher Feedback: The teacher groups were run in smaller sessions, which allowed for immediate feedback integration and content modification. This iterative, teacher-centered design process proved highly effective. Teachers identified several areas for improvement in the curriculum, including:

- **Age-Appropriate Language**: Adjusting vocabulary and phrasing to better suit different K-5 grade levels.
- **Missing Steps in Activities**: Clarifying instructions for activities, as some initial assumptions about teacher actions needed explicit detailing.
- **Typos and Errors**: Correcting minor errors in the materials.
- **Difficulty Level Adjustment**: Reallocating certain content between different grade levels based on observed difficulty.
- **Online Assessment**: Providing an option for online assessments instead of paper version for different lessons.
- **Internet Safety Standards**: Mapping the standards to the ISTE Computer Science and Cybersecurity standards instead of one state.

After each round of testing, the curriculum was promptly modified, and the revised content was then tested with the subsequent teacher group. This iterative refinement process ensured that the materials were highly usable and practical for classroom implementation by teachers.

Cybersecurity Expert Consultation: The consultations with over 20 cybersecurity experts, encompassing university professors, researchers,

and industry/IT security professionals, validated the critical need for cybersecurity education at the K-5 level. Experts provided comprehensive feedback on the curriculum's content, emphasizing the importance of including foundational concepts and identifying key areas for future workforce development that should begin in elementary schools. Their insights were instrumental in shaping the overall materials for both students and teachers, ensuring the curriculum's relevance and alignment with current industry needs and future trends. They also provided guidance on effective modalities for delivering training to both teachers and students.

7. DISCUSSION

The empirical evaluations of the Cyber-PARK initiative, involving K-5 students, teachers, and cybersecurity experts, strongly demonstrate its efficacy and critical importance. Student responses highlighted the power of gamified and hands-on learning, with pre- and post-assessments confirming improved comprehension, aligning with the "knowing is doing" principle of situated cognition theory.

The iterative design process, heavily informed by K-5 teacher feedback, was crucial for developing a practical and user-friendly curriculum. This teacher-centered approach allowed for immediate adjustments to language, activity instructions, and content difficulty, ensuring the materials are highly usable and address the challenge of limited teacher training in cybersecurity.

Furthermore, strong endorsement from academic and industry cybersecurity experts validated the curriculum's content and its alignment with broader cybersecurity workforce development goals. Their input ensures Cyber-PARK is academically sound and relevant, contributing significantly to building a skilled talent pipeline by starting education at the elementary level.

Unlike many current passive or overly complex cybersecurity education offerings for young children, Cyber-PARK stands out by actively integrating gamified learning with comprehensive, standards-aligned content and built-in assessment opportunities. Detailed data from games like Potion Post, Password Chef, and Two-Step Treasures provides measurable outcomes, addressing a significant limitation in existing programs. Ultimately, Cyber-PARK directly combats educational inequality and promotes digital inclusion, fostering responsible digital citizenship and reducing vulnerability to cyber threats on a societal scale.

8. CONCLUSIONS

Cybersecurity education is indispensable for empowering young learners to navigate the digital world safely and responsibly. The Cyber-PARK project directly addresses this need by providing an innovative, empirically validated platform for K-5 students, teachers, and parents. By reducing children's vulnerability to online threats such as fraud, scams, and identity theft, early cybersecurity education fosters a generation of informed and cautious digital citizens.

Through the development and refinement of engaging, interactive games and a comprehensive curriculum, we aim to make learning these critical concepts both accessible and enjoyable. The positive feedback and demonstrated comprehension from students, the iterative refinement based on teacher insights, and the expert validation of the content collectively affirm the strength and relevance of the Cyber-PARK approach. By combining research-driven educational methods with hands-on experiences, we strive to create a lasting impact, empowering children to build safe digital habits that will benefit them throughout their lives.

9. FUTURE WORK

The Cyber-PARK project is being piloted in New Hanover County public elementary schools. This large-scale pilot will provide a rich, longitudinal database encompassing all activities and content within the curriculum. This includes detailed data on PowerPoint presentations used by educators, in-class activities, student engagement with video games, assessment sheets, and take-home exercises. This extensive data collection will allow for a more robust empirical analysis of the curriculum's long-term impact on student learning, behavior, and interest in cybersecurity. The future work will focus on:

- *Longitudinal Impact Assessment:* Analyzing the data from the pilot program to understand the sustained effects of Cyber-PARK on students' cybersecurity knowledge, attitudes, and behaviors over time.
- *Curriculum Expansion and Refinement:* Continuously developing new interactive games and learning modules based on evolving cyber threats and educational needs, while further refining existing content through ongoing feedback loops.
- *Teacher Training and Support:* Developing scalable teacher training programs and

support resources to facilitate widespread adoption and effective implementation of the Cyber-PARK curriculum.
- Integration with Existing Educational Frameworks: Ensuring seamless integration of Cyber-PARK with existing school curricula and educational technology infrastructures.
- Age-Related Content: Revisiting the lessons and student's activities and reevaluating their age appropriateness.

Through these ongoing efforts to establish Cyber-PARK as a leading solution for early cybersecurity education, contributing significantly to a more cyber-resilient and digitally literate future generation.

11. REFERENCES

Acton, R. (2023). Doing knowledge work differently: Problem-based projects as encounters in coming-to-know. *Higher Education*, *86*(1), 225-242.

Anderson, M., & Jiang, J. (2018). Teens, social media & technology 2018. *Pew research center*, *31*(2018), 1673-1689.

Anggraeni, D. M., Prahani, B. K., Suprapto, N., Shofiyah, N., & Jatmiko, B. (2023). Systematic review of problem based learning research in fostering critical thinking skills. *Thinking Skills and Creativity*, *49*, 101334. https://doi.org/10.1016/j.tsc.2023.101334

Cabual, R. A. (2021). Learning styles and preferred learning modalities in the new normal. *Open Access Library Journal*, *8*(4), 1-14. 10.4236/oalib.1107305.

Felder, R. M. (2020). Opinion: Uses, misuses, and validity of learning styles. *Advances in Engineering Education*, *8*(1), 1-16.

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security*, *100*, 102080. https://doi.org/10.1016/j.cose.2020.102080

Giannakas, F., Papasalouros, A., Kambourakis, G., & Gritzalis, S. (2019). A comprehensive cybersecurity learning platform for elementary education. Information Security Journal: A Global Perspective, 28(3):81–106. https://doi.org/10.1080/19393555.2019.1657527

Han, I. (2020). Immersive virtual field trips in education: A mixed-methods study on elementary students' presence and perceived learning. British Journal of Educational Technology, 51(2), 420-435. https://doi.org/10.1111/bjet.12842

Höfrová, A., Balidemaj, V., & Small, M. A. (2024). A systematic literature review of education for Generation Alpha. *Discover Education*, *3*(1), 125.

ISC2 Cybersecurity Workforce Study (2023). How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce, https://cybergovernancealliance.org/wp-content/uploads/2024/01/ISC2_Cybersecurity_Workforce_Study_2023-1.pdf

Jethwani, M., Memon, N., Richer, A., and Seo, W. (2016). It's hard to be the only girl: Obstacles facing adolescent girls in computer science contexts. In Journal of The Colloquium for Information System Security Education, volume 4, pages 16–16. https://cisse.info/journal/index.php/cisse/article/view/52

Jethwani, M. M., Memon, N., Seo, W., and Richer, A. (2017). "I can actually be a super sleuth" promising practices for engaging adolescent girls in cybersecurity education. Journal of Educational Computing Research, 55(1):3–25. https://doi.org/10.1177/0735633116651971

Kim, S., Song, K., Lockee, B., & Burton, J. (2017). What is gamification in learning and education? In *Gamification in learning and education: Enjoy learning like gaming* (pp. 25-38). Cham: Springer International Publishing.

Kodey, A., Bedard, J., Nipper, J., Post, N., Lovett, S., & Negreros, A. (2023). The US needs more engineers. What's the solution?. *Boston Consulting Group*, *13*.

MacIsaac, D. (Ed.). (2019). US government releases charting a course for success: America's strategy for STEM education, report guiding federal agencies that offer STEM funding opportunities. The Physics Teacher, 57(2), 126-126. https://doi.org/10.1119/1.5088484

Mikrouli, P., Tzafilkou, K., & Protogeros, N. (2024). Applications and learning outcomes of game based learning in education. International Educational Review, 2(1), 25-54. https://doi.org/10.58693/ier.212

Mumtahana, L., Rosyidah, C. N., Kausar, S., Khamim, N., & Syamsi, M. (2026). Teachers' Efforts to Implement Problem-Based Learning

in Order to Improve Students' Collaboration and Communication Skills. At-Tadzkir: Islamic Education Journal, 5(1), 101-113. https://doi.org/10.59373/attadzkir.v5i1.181

National Science Teaching Association (2020), Position Statement. *STEM Education Teaching and Learning*. National Science Teaching Association, February 2020.

National Science Foundation (2020). Cybersecurity education in the age of artificial intelligence. https://www.nsf.gov/pubs/2020/nsf20072/nsf20072.jsp.

Nemakhavhani, R. B. (2024, November). Enhancing student engagement through problem-based learning: A case of the built environment. In *International conference on education research* (Vol. 1, No. 1, pp. 238-245).

Onoshakpokaiye, O. E., & Avwiri, H. E. (2025). Science, technology and mathematics education: A roadmap to economic growth and sustainable development of the developing nations. *Indonesian Journal of Education and Mathematical Science*, *6*(2), 59-69. https://doi.org/10.30596/ijems.v6i2.23902

Ortiz-Rojas, M., Chiluiza, K., & Valcke, M. (2019). Gamification through leaderboards: An empirical study in engineering education. *Computer Applications in Engineering Education*, *27*(4), 777-788. https://doi.org/10.1002/cae.12116

Parthasarathy, P. K., Mittal, A., & Aggarwal, A. (2023). Literature review: Learning through game-based technology enhances cognitive skills. *International Journal of Professional Business Review: Int. J. Prof. Bus. Rev.*, *8*(4), 29.

Pflieger, L. C. J., Hartmann, C., & Bannert, M. (2024). Enhancing knowledge construction in emerging technologies: The role of imagination training in immersive virtual reality environments. Discover Education, 3(1), 65.

Putz, L.-M., Hofbauer, F., and Treiblmaier, H. (2020). Can gamification help to improve education? Findings from a longitudinal study. Computers in Human Behavior, page 106392. https://doi.org/10.1016/j.chb.2020.106392

Quayyum, F., Cruzes, D. S., and Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. International Journal of Child-Computer Interaction, Volume 30:100343. https://doi.org/10.1016/j.ijcci.2021.100343

Szymkowiak, A., Melović, B., Dabić, M., Jeganathan, K., & Kundi, G. S. (2021). Information technology and Gen Z: The role of teachers, the internet, and technology in the education of young people. *Technology in society*, *65*, 101565. https://doi.org/10.1016/j.techsoc.2021.101565

Xu, E., Wang, W., & Wang, Q. (2023). The effectiveness of collaborative problem solving in promoting students' critical thinking: A meta-analysis based on empirical literature. Humanities and Social Sciences Communications, 10(1), 16.

Xu, Y., & Li, H. (2025). Cybersecurity matters for primary school students: A scoping review of the trends, challenges, and opportunities. *IEEE Transactions on Learning Technologies, 18, 513-529. 10.1109/TLT.2025.3564610*

Zaza, S., Abston, K., Arik, M., Geho, P., & Sanchez, V. (2020). What CEOs have to say: Insights on the STEM workforce. *Zaza, Sam*, 136-155.

APPENDIX A

Detailed module content for K-5, mapped to the NC K-12 Computer Science Standards.

Module 1: Digital Foundations

- ***Devices:*** Understand basic digital elements.
- ***Network & Internet:*** How things connect.
- ***Accounts & Passwords:*** Basic security concepts.
- ***Digital Footprints:*** What we leave behind online.

NC K-12 Computer Science Standards

- **K2-NI-01:** Illustrate how information is broken down into smaller pieces and can be reassembled.
- **K2-NI-02:** Apply knowledge of what passwords are and why we use strong passwords to protect devices and information from unauthorized access.
- **K2-NI-03:** Discover and understand what a digital footprint is, and how information can be obtained and protected.
- **K2-IC-04:** Model responsible login and logoff procedures on all devices
- **68-IC-09:** Compare tradeoffs between allowing information to be public and keeping information private and secure.

Computing Device	**K2-NI-02, K2-DA-02**: Physical items that use hardware and software to receive, process, and output information. Computing, inputting, networking, and peripheral are all examples of devices.
USB	A standard interface for connecting cables to PCs and consumer electronics devices. Users can connect a specially designed wire called the USB cable. USB cables may transmit both power and information
HDMI	A connection used for displaying digital video and audio from a source, such as a computer or TV, to a computer monitor, TV or projector.
Bluetooth	a short-range wireless connection of mobile phones, computers, and other electronic devices to exchange data.
Cell Tower	Cell towers are structures that house the equipment necessary for wireless communication between phones that allow us to make calls, exchange text messages, and access the internet on mobile devices.
Wifi and Hotspots	a wireless networking technology that uses radio waves to provide wireless high-speed Internet access.
Internet	**35-NI-01**: The large system of connected devices around the world that allows people to share information and communicate with each other.
Network	**35-NI-01, ICS-NI-01:** A collection of computers that are connected together so that they can share information.
Router	**ICS-NI-01:** A router is a unique electronic device that allows the network to be shared with people in a small area.
Browser	A browser is an application on a device that connects to the internet and allows you to view and interact with the information on it.
Account	A user's access to a specific Internet platform. An account contains a variety of personal and private information used to interact with others online.
Password	**K2-NI-02**: A string of characters used for authenticating a user on a computer system. Most passwords are comprised of several characters, which can typically include letters, numbers, and most symbols, but not spaces.
Digital Footprint	**K2-NI-03, 35-NI-02:** A trail of data you create while using the Internet. It includes the websites you visit, emails you send, and information you submit to online services.

	A "passive digital footprint" is a data trail you unintentionally leave online. (example IP address, browsing history, ...) An "active digital footprint" includes data that you intentionally submit online. (example email, social media post, ...)
Digital Citizenship	**35-IC-04:** The norms of appropriate, responsible behavior with regard to the use of technology. Digital citizenship topics include instruction on media balance, privacy and security, cyberbullying, news and media literacy, and digital identity and footprint.

Module 2: Online Protections

- ***Password Building:*** Strategies for strong, memorable passwords.
- ***Social Etiquette:*** Positive online interactions.
- ***Malicious Actors:*** Understanding who poses threats.
- ***Password Cracking (Basics):*** How weak passwords are vulnerable.

NC K-12 Computer Science Standards

- **68-NI-02:** Explain how physical and digital security measures protect electronic information
- **68-NI-03:** Explain permission and authorizations to access resources to computer systems online
- **K2-IC-03**: Work respectfully and responsibly with others online
- **35-IC-04:** Exhibit positive digital citizenship and social responsibility in online interactions
- **ICS-NI-02:** Identify examples to illustrate how sensitive data can be affected by malware and other attacks.

Digital Citizenship	**35-IC-04:** The norms of appropriate, responsible behavior with regard to the use of technology. Digital citizenship topics include instruction on media balance, privacy and security, cyberbullying, news and media literacy, and digital identity and footprint.
Password Cracking	The process of guessing passwords protecting a computer system or account. Generally done through brute-force.
Netiquette	A set of guidelines in online communication that help to ensure positive interactions.
Malicious Actors	a person or a group of people that take part in an action that is intended to cause harm to the individuals or companies using: computers, devices, systems, or networks
Password	**K2-NI-02**: A string of characters used for authenticating a user on a computer system. Most passwords are comprised of several characters, which can typically include letters, numbers, and most symbols, but not spaces.
Netiquette	The set of rules and behaviors that people are expected to use when interacting with others on the internet.
Phishing	The practice of sending fraudulent communications that appear to come from a legitimate and reputable source, usually through email and text messaging.
Malware Ads	The use of malicious code in online ads and popups to spread malware or steal information. Scammers use them as a covert tactic to spread dangerous code across multiple websites.
Social Engineering	The tactic of manipulating, influencing, or deceiving someone to gain control over a computer system or to steal personal and financial information.

Module 3: Threat Identification

- ***Multi-Factor Authentication (MFA):*** Adding layers of security.
- ***Phishing: Identifying*** online scams.
- ***Catching Misinformation:*** Critical evaluation of online content.
- ***Cyberbullying:*** Identifying and reporting.

NC K-12 Computer Science Standards

- **68-NI-04:** Apply multiple methods of encryption to model the secure transmission of information.
- **68-NI-02:** Explain how physical and digital security measures protect electronic information.
- **35-IC-04:** Exhibit positive digital citizenship and social responsibility in online interactions.
- **68-IC-08:** Understand how online interactions make an impact on the social, emotional, and physical aspect of others.

One-Time Password	an automatically generated password that is only valid for a single login session or transaction.
Multi-factor authentication	an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more distinct types of evidence (or factors) to an authentication mechanism.
Authentication Factor	a special category of security credential that is used to verify the identity and authorization of a user attempting to gain access, send communications, or request data from a secured network, system or application.
Phishing	Phishing is the practice of sending fake communications that appear to come from a legitimate and reputable source, usually through email and text messaging.
Electronic mail (email)	a communication method that uses electronic devices to deliver messages across computer networks. "Email" refers to both the delivery system and individual messages that are sent and received.
Chat Messaging	Chat messages are instant digital communications exchanged over the internet through various platforms like live chat, social media, and messaging applications.
Bias	a tendency to believe that some people, ideas, etc., are better than others, which often results in treating some people unfairly.
Cyberbullying	the use of technology to harass, threaten, embarrass, or target another person. Online threats and mean, aggressive, or rude texts, tweets, posts, or messages all count. So does posting personal information, pictures, or videos designed to hurt or embarrass someone else.
Misinformation	False or Incorrect information. It is usually done accidentally.
Disinformation	Intentionally incorrect information meant to mislead individuals or the general public.
CAARP method	A 5-step method used to identify misinformation. They are: - Currency: When was this made? Is it out of date? - Authority: Are they an expert on the topic? - Accuracy: Where did their information come from? - Relevance: Is the information useful to you? Purpose: What is the intention behind it?

Module 4: Future & Responsibility

- ***How Technology Evolves:*** Introduction to Deepfakes & AI.
- ***Careers in Cybersecurity:*** Pathways for future professionals.
- ***Safety in Numbers:*** Responsible Digital Citizenship.
- ***Maintaining Digital Habits:*** Lifelong online safety.

NC K-12 Computer Science Standards

- **35-IC-01:** Compare computing technologies that have changed the world and how they both influence and are influenced by cultural practices.
- **ICS-NI-02:** Identify examples to illustrate how sensitive data can be affected by malware and other attacks.

Artificial Intelligence	Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
Machine Learning	A program that uses data and algorithms to train computers to make classifications, generate predictions, or uncover similarities or trends across large datasets.
Generative AI	Deep-learning models that can generate high-quality text, images, and other content based on the data they were trained on.
Deepfake	an image, video, or audio that has been edited or generated using artificial intelligence.
Career	an occupation or profession, especially one requiring special training
Information Security Analyst	A career where individuals monitor and maintain networks, making sure company data stays safe and secure.
Digital Forensic Examiner	A professional who analyzes digital evidence in legal or criminal investigations.
Pen Tester	A cybersecurity professional who simulates cyberattacks on computer systems, networks, and applications to identify and exploit vulnerabilities.
Security Architect	A professional who designs, builds, and implements security systems within an organization's IT infrastructure. They are responsible for safeguarding networks, data, and information from cyber threats and ensuring compliance with security policies and standards.
Cryptography Engineer	A career where a professional designs, develops, implements, and analyzes cryptographic algorithms and systems to secure data and communication. They work with software and hardware to integrate these systems into various applications, devices, and networks.