2026 ASEE ANNUAL CONFERENCE June 21–24, 2026 | Charlotte Convention Center, NC
Host Sponsor UNC Charlotte
ASEE AMERICAN SOCIETY FOR ENGINEERING EDUCATION
Paper ID #53898

EML in Network Security: Cultivating Curiosity, Connections, and Value in Cybersecurity Education

Dr. M Ajmal Khan, Ohio Northern University

Dr. Khan is an Associate Professor in the Electrical & Computer Engineering and Computer Science Department at Ohio Northern University (ONU), Ohio, US. He completed his Ph.D. in Wireless Security and Data Networks. He has taught courses in the areas of Cybersecurity, Computer Networks, Network Security, Penetration Testing, and Wireless and Communication Networks. His research focuses on Cybersecurity, IoT Security, Machine Learning, Relay Networks, and Physical Layer Security. His successes include more than 35 refereed publications. In addition, he is a member of ASEE, IEEE, and ISC2, and he holds CompTIA Security+, ISC2 CC, and Cisco CCNA Certifications.

EML in Network Security:
Cultivating Curiosity, Connections, and Value in Cybersecurity Education

Abstract

This paper presents an empirical study on cultivating Entrepreneurially Minded Learning (EML) into a senior-level Network Security course. The study explains the integration of the entrepreneurial mindset into a technically focused network security curriculum, which is centered on curiosity, connections, and value creation. Three structured instructional modules were developed, which were grounded in client-driven security solution design, prototype implementation, and ethical-professional reasoning. In addition, these three modules were implemented and assessed using Expanded KEEN Student Outcomes (eKSOs). Quantitative assessment results prove strong student achievement across all targeted outcomes, with no students performing below adequate levels. The results show that EML can be incorporated into network security education without sacrificing the technical depth of the course, while significantly enhancing students' professional readiness and entrepreneurial thinking.

1. Introduction

Entrepreneurially Minded Learning (EML) has emerged as a game-changing pedagogical paradigm in engineering education, fostering the entrepreneurial mindset (EM) of curiosity, interdisciplinary connections, and value creation among students, in addition to improving technical skills [1] [2] [3]. In today's digital economy, organizations are heavily dependent on robust, secure, and adaptable network infrastructures. Thus, network engineers having both strong technical skills and an entrepreneurial mindset are in growing demand [4]. With an EM mindset, network engineers can follow opportunities, navigate ambiguity, and deliver solutions that create value for clients, in addition to designing, securing, and managing complex networks [5].

Typically, network security education has often focused on mastering protocols, configurations, and security algorithms to address emerging threats [6]. While these skills are still vital, contemporary industry expectations go far beyond technical proficiency [7]. Employers and businesses now emphasize that the graduates should possess skills to identify new problems, balance trade-offs, communicate value propositions, and make decisions with ethical and entrepreneurial considerations [8] [9]. The skill to combine engineering rigor with the EM can be seen as a differentiation in hiring the workforce [10].

Cyber threats are becoming increasingly sophisticated due to Artificial Intelligence (AI) [11] [12], requiring future cyber professionals to approach their work with both technical and entrepreneurial skills. Thus, future professionals need to provide innovative solutions to tackle the latest security challenges. For this purpose, future professionals should be able to identify opportunities within constraints, adapt rapidly to new threat landscapes, and envision new methods for creating value and ensuring trust in digital systems [13]. This combination of cybersecurity and entrepreneurship is now becoming critical for training current students to meet the demands of organizations and society at large [14].

This paper details the systematic integration of EML principles into a senior-level Network Security course (ECCS 4321) offered for Computer Engineering and Computer Science programs at Ohio Northern University (ONU). The course is structured to serve students in computer engineering and computer science, and is intentionally designed to bridge the gap between technical mastery and entrepreneurial capability. Leveraging experiential learning, client-driven projects, and ethical reflection, the course aims to cultivate the "3Cs" of the entrepreneurial mindset: curiosity, connections, and creating value. Students complete three core modules in this course: Network Security Solution, Ethical and Professional Responsibilities, and Entrepreneurially Minded Security Design. These modules include real-world scenarios with hands-on technical exercises. In addition, these modules engage students in decision-making processes that introduce opportunity recognition, client perspectives, and ethical responsibilities.

This manuscript presents the course structure, pedagogical strategies, assessment methods, and resulting student outcomes, providing an empirical model for embedding EML in cybersecurity education. The results demonstrate that integrating EML principles into the curriculum not only maintains technical rigor but also significantly enhances students' ethical awareness, professional preparedness, and entrepreneurial capacity. This approach prepares computer engineering and computer science graduates to excel in the dynamic, opportunity-rich landscape of modern network security and cybersecurity.

2. Background and Literature Review

The high shortage of cybersecurity professionals remains a big challenge for both industry and higher education, with forecasts predicting continued gaps in workforce supply relative to demand [7]. The current cybersecurity roles need adaptability, innovative problem-solving, and the ability to make value-driven judgments in complicated and dynamic settings, in addition to deep technical expertise [9]. Thus, Entrepreneurially Minded Learning (EML) has gained importance as a comprehensive pedagogical approach in engineering education [1] [10] [15], and it is also strongly advocated by the Kern Entrepreneurial Engineering Network (KEEN). EML is based on promoting curiosity to pursue alternative solutions, building connections to integrate multidisciplinary knowledge, and cultivating the capacity to create value for organizations and society [15] [16] [17].

Traditional cybersecurity curricula have primarily stressed technical content, such as protocols, system configurations, and threat mitigation. However, it is often insufficient to develop a professional, ethical, and entrepreneurial mindset (EM) in students [18]. Therefore, recent research highlights the value of introducing experiential, project-based, and client-driven learning experiences to prepare students [19] [20]. Project-Based Learning (PBL) approaches have proven to be successful in improving student engagement, strengthening transferable skills, and increasing workforce readiness [21] [22] [23].

In addition, ethical education in computing is now widely regarded as essential to the professional formation of engineers and computer scientists [24]. Introducing ethical reflection and reasoning within a cybersecurity course prepares students to recognize societal, legal, and ethical situations of their work and to make informed decisions [25]. Integrating ethics into EML

frameworks reinforces the imperative of value creation not only in economic terms, but also in its societal and ethical impact.

Thus, EML is embedded into a network security course to prepare students for hybrid technical and entrepreneurial roles in an evolving workforce. This manuscript builds on the foundation established by the prior engineering education work. In addition, this manuscript provides empirical evidence of EML in cybersecurity education, specifically through the use of the project-based, ethically integrated technical curricula.

3. Course Context and Structure

Network Security is a three-credit, senior-level elective course, which is designed to prepare students from electrical engineering, computer engineering, and computer science programs, particularly the cybersecurity minor. The course cultivates a multidisciplinary learning environment that mirrors the collaborative nature of the cybersecurity profession.

The course covers a wide range of topics necessary for network security professionals. The topics include Virtual LANs (VLANs), Network Address Translation (NAT), Access Control Lists (ACLs), AAA protocols, IPsec, VPNs, ASA and zone-based firewalls, Demilitarized Zone (DMZ), and intrusion prevention systems (IPS). In this course, students engage in a combination of formal lectures, hands-on lab exercises utilizing Cisco Packet Tracer and physical lab equipment, and open-ended projects that simulate real-world scenarios. The experiential and project-based nature of this course makes it stand out among other courses. Each module of this course includes hands-on projects that require students to design, configure, test, and troubleshoot network security solutions. In addition, the course purposefully incorporates consultant-client interactions, solution development, and structured ethical reasoning, thereby simulating the complications of professional practice.

The course was redesigned to integrate EML across three instructional modules without removing any technical content. These modules are aligned with Expanded KEEN Student Outcomes (eKSOs) [26] and the 3Cs framework: curiosity, connections, and creating value. This modular structure purposefully guides students from design to implementation, and finally to ethical reflection.

4. Entrepreneurially Minded Learning Modules

The EM mindset is integrated into the Network Security course, which was structured around three integrated EML modules: (1) Network Security Solution for a Client, (2) Developing a Network Prototype with Security Requirements, and (3) Ethical and Professional Responsibilities of a Network Security Specialist. These modules were developed to incorporate the EML principles of curiosity, connections, and creating value into the cognitive, technical, and professional areas, thus improving students' learning.

Rather than treating entrepreneurial thinking as an add-on or isolated activity, the modules were intentionally sequenced to mirror professional practice in cybersecurity. First, students perform

an exploratory problem modelling and client-centered design. Second, students' progress toward technical implementation and validation. Finally, students reflect on the ethical and societal impacts of cybersecurity decision-making. This integrated structure enables students to experience cybersecurity not only as a technical discipline, but also as a value-driven, client-oriented professional practice.

4.1 Module 1: Network Security Solution for a Client

In this module, students are getting acquainted with a consultancy-style environment that reflects professional cybersecurity practice. In the managed cybersecurity services (MSPs) industry, network security specialists often serve as consultants, translating client needs, evaluating technical alternatives, and proposing feasible solutions. This module was designed to provide a simulated, real-world environment in which a network security consultant responds to an open-ended client request.

At the beginning of the module, students are presented with a client advertisement that describes requirements, organization structure, and security expectations of a fictional company. In the advertisement, the technical specifications were deliberately omitted to encourage students to immerse themselves in inquiry-driven exploration. This ambiguity triggers students' curiosity, motivating them to ask questions about network size, business operations, geographic distribution, security priorities, scalability, and future expansion needs.

Working in small consulting teams, students develop an initial network security solution that includes a logical network architecture and the selection of appropriate security technologies. Students are encouraged to explore alternatives for routing protocols, firewalls, access control mechanisms, virtual local area networks (VLANs), authentication services, and encryption methods. This process motivates students to explicitly establish connections between theory and the application of enterprise network design.

Students design a decision metric, which is a central component of this module. In addition, students design a criterion, such as performance, cost, scalability, manageability, and security effectiveness. Moreover, students use the decision metric to convince the client of their design decisions. Thus, this requirement shifts the focus from a single correct solution to evaluating design and business trade-offs. Eventually, this requirement reinforces entrepreneurial thinking and trains students to articulate rationale in a client-centered context.

Students engage in iterative interaction with the client to ask questions and seek clarification, where the client is represented by the course instructor. A professional meeting and communication with the client (i.e., the instructor) are organized, which gives students an opportunity to clarify assumptions, discuss decisions, and revise their solutions in line with the client's expectations. This iterative process reinforces curiosity through continuous questioning and responding, which strengthens connections between technical knowledge and stakeholder needs. In addition, this process emphasizes the importance of communicating temporary results rather than just presenting the final design.

After completing Module 1, students have developed a finalized security solution that primarily meets the client's requirements. In addition, students engage in informed decision-making and professional communication, which ultimately provides a groundwork for technical implementation.

Readers and interested instructors are referred to [27] for a comprehensive account of Modules 1 and 2, including the full assignment description, assessment rubrics, course syllabus, and representative samples of student work. The syllabus explicitly outlines all course topics, learning objectives, and alignment with ABET student outcomes. It also demonstrates that integrating elements of the entrepreneurial mindset (EM) does not compromise the course's technical rigor. As detailed in [27], EM is incorporated through project-based activities completed outside of scheduled class time.

4.2 Module 2: Developing a Network Prototype with Security Requirements

Once students have successfully developed a plan and framework for the client's security solution, they shift their focus to building a functional network prototype in the second module. The second module put more emphasis on the EM mindset of creating value. Students develop the network prototype to implement their proposed security solution using a network simulator, primarily Cisco Packet Tracer. While a physical deployment of an enterprise network is not feasible in an academic laboratory, students rely on simulation to set up a realistic network model. In addition, students perform testing and troubleshooting that closely approximate a real-world environment.

Students configure routing protocols on Cisco Routers, implement firewall policies on Cisco ASA firewalls, apply access control lists on routers and firewalls, set up virtual private networks (VPNs), deploy authentication mechanisms, and implement other security measures, as approved by the client in their final security solution. When students start the development process in Cisco Packet Tracer, which mimics real-world network components, they face real-world challenges with configuration and troubleshooting.

This module strengthens connections to integrate knowledge across multiple courses, rather than treating security techniques as isolated tools. In addition, this module reinforces curiosity when students test their network solutions, identify security gaps, and troubleshoot network configurations to improve the security posture. Students experience firsthand that value is not created solely through innovative ideas, but through solutions that can be implemented, tested, and validated in a real-world environment. The process students experienced in this module reflects and prepares students for a professional cybersecurity environment, where successful solutions must function under operational conditions rather than exist only as conceptual designs.

After completing this module, students gain a deeper experience of the relationship between a design reported on paper and implementation communicated through a network simulator. This module also strengthens students' ability to deliver practical, value-oriented cybersecurity solutions.

4.3 Module 3: Ethical and Professional Responsibilities of a Network Security Specialist

The third module addresses the ethical and professional aspects of cybersecurity professionals, and stresses that the EM mindset must be grounded in responsibility as well as societal awareness. As students learn advanced skills in the network security course, such as network monitoring, packet capturing, access control, and encryption, they gain the power to impact privacy, integrity, and trust. Thus, this module was specifically designed to help students realize their responsibilities.

This module introduces students to ethical scenarios commonly encountered by cybersecurity professionals, including unauthorized monitoring, misuse of administrative privileges, insider threats, data privacy violations, and responsible vulnerability disclosure. The instructor leads several guided discussions in class and uses real-world scenarios that present various examples and situations to discuss tensions among organizational goals, legal obligations, and ethical standards. These discussions encourage students to analyze consequences, consider multiple stakeholders, and evaluate long-term impacts of technical decisions. This thoughtful conversation among students and with the instructor in class supports the EML principle of creating value by broadening students' understanding of value beyond technical performance to include societal, professional, and human considerations.

This module reinforces connections between cybersecurity practice and professional identity. Students are encouraged to consider themselves as trusted professionals whose decisions influence organizational resilience, customer confidence, and public safety. When students realize and consider themselves in such a trustworthy position, they learn to integrate moral judgment directly into technical education.

After completing this module, students learn about their critical role in society and how to remain ethical, responsible, and aligned with professional standards.

Readers and interested instructors are referred to [28] for comprehensive details on Module 3, including the full assignment description and assessment rubrics.

5. Learning Outcomes and Assessment Methods

The EML framework implemented in this course is based on the Expanded KEEN Student Outcomes (eKSOs) [26]. The eKSOs employ a structured, measurable approach to assess the EM mindset in engineering and computing education. This network security course explicitly maps learning outcomes to each EML module. This mapping confirms that the EM mindset is purposely embedded in network design, configuration, implementation, and troubleshooting activities to evaluate student learning using measurable artifacts in these EML modules. The learning outcomes for this study are well aligned with the best practices of network security professionals. These learning outcomes encourage students to consider alternative solutions, deliver working models that meet requirements, and exercise ethical judgment. In addition, each outcome is aligned with one of the three EML modules and is assessed through measurable student artifacts such as a network model, report, or reflection.

5.1 Alignment of Learning Outcomes with EML Modules

Each EML module was designed to emphasize a specific aspect of the EM mindset while reinforcing technical learning objectives. Learning outcomes were purposely selected and designed to align with the nature of activities within each module and the types of professional skills being developed.

- Module 1 emphasizes curiosity and analytical decision-making as students explore multiple security solutions and justify their final proposed solution using a decision metric.
- Module 2 emphasizes creating value through implementation, as students translate conceptual security solutions into functional network security prototypes.
- Module 3 emphasizes ethical awareness and professional character as students examine their societal and professional responsibilities in cybersecurity and network security.

This learning outcomes mapping enables a clear progression from inquiry and exploration to execution and validation, and finally to reflection and ethical study.

5.2 Module 1 Learning Outcome and Assessment Artifacts

The following learning outcome for Module 1 centers around enabling students' curiosity through the exploration of alternative network security solutions. In addition, students are required to identify multiple network security techniques, algorithms, and design strategies. Moreover, students investigate their proposed alternatives related to routing protocols, firewall configurations, access control mechanisms, authentication protocols, and network segmentation. Then, students develop decision metrics to compare options based on relevant criteria such as security effectiveness, performance, scalability, cost, and maintainability.

eKSO 1-i (Curiosity): Develop multiple techniques for network security, and create and apply decision metrics.

Student learning for this outcome is assessed using artifacts produced during the design phase of the client-based project, including:

- Project proposal documents describing the conceptual network security solution
- Decision metrics to compare alternative solutions
- Explanation to justify their selected solution

These artifacts provide measurable evidence that shows students have acquired the ability to explore multiple alternatives, apply analytical reasoning, and make informed decisions in response to open-ended problems.

5.3 Module 2 Learning Outcome and Assessment Artifacts

This learning outcome for Module 2 focuses on the EML principle of creating value through hands-on application and execution. Once the proposed security solution, Module 1, is approved,

students move from design to hands-on implementation. Students develop a working model of the network security prototype using Cisco Packet Tracer. In addition, students' ability to apply their design decisions and demonstrate that the proposed security solution can function under the client's requirements and realistic conditions. Moreover, students configure routing protocols, firewalls, VPNs, authentication protocols, and access control mechanisms in accordance with client requirements.

eKSO 3-c (Creating Value): Create a network security model that meets the requirements of the client.

Student achievement of this outcome is evaluated using an implementation-based network model, including:

- Network simulation files developed using Cisco Packet Tracer
- Configuration documentation for routers, switches, and security devices
- Evidence of the working model, aligned with the client's requirements and best security practices.

This network model serves as an artifact for measuring students' performance on this outcome. This shows that students have acquired the ability to translate design into a working model and to deliver solutions that provide technical value.

5.4 Module 3 Learning Outcome and Assessment Artifacts

This learning outcome of Module 3 addresses the ethical and professional responsibilities associated with cybersecurity and network security careers. Students must also understand the consequences of misuse, negligence, or unethical decision-making. This outcome measures students' skills to analyze ethical and professional issues, consider multiple stakeholders, and evaluate the broader implications of cybersecurity actions. Scenarios explored in this module include issues related to privacy, surveillance, insider threats, data misuse, and responsible vulnerability disclosure.

eKSO 6-c (Character): Recognize and evaluate potential impacts while making informed ethical and professional decisions.

The assessment of this outcome was performed using a set of scenario-based multiple-choice questions in the final exam. These MCQs are based on various real-world scenarios to measure students' understanding of this module.

6. Results and Discussion

This section presents and discusses the empirical results for the three eKSOs, which align with the EML modules incorporated into the Network Security course. Student artifacts to measure students' performance include project proposals, decision-metric analyses, network simulation files, and final examination MCQs. Students' performance was analyzed using a categorical scale, EAMU (Excellent, Adequate, Minimal, Unsatisfactory), which is represented using a

percentage scale as Excellent (≥90%), Adequate (75–89%), Minimal (60–74%), or Unsatisfactory (<60%). In addition, the data was visualized in pie charts for each module. The purpose of this analysis is to report students' performance levels and examine the effectiveness of the EML framework in a technically intensive, application-intensive network security course.

6.1 Results for Module 1: Client-Based Network Security Solution (eKSO 1-i)

The outcome eKSO 1-i for Module 1 measures students' ability to develop multiple techniques for network security and apply decision metrics to justify their security solutions. This outcome is perfectly in line with the EM mindset regarding curiosity, which emphasizes inquiry, exploration of alternative solutions, and analytical reasoning.

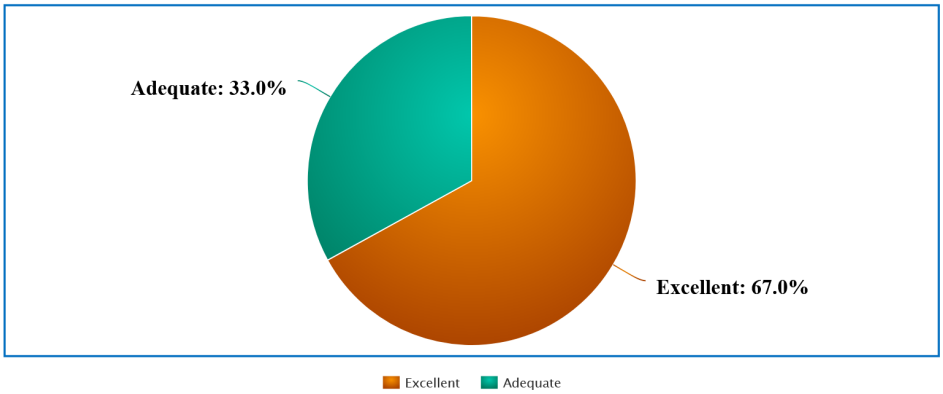

Figure 1: Student Performance in Module 1, eKSO 1-i (Curiosity).

The data is shown in Figure 1, which indicates that 67% of students achieved an Excellent performance level, while the remaining 33% achieved an Adequate level. Note that no students were categorized as Minimal or Unsatisfactory, which strongly indicates that all students demonstrated at least acceptable competency in evaluating and justifying network security decisions. In addition, the results show strong student skills in solving open-ended problems and analyzing comparative studies.

Students demonstrated the ability to move beyond single-solution thinking by exploring multiple routing protocols, security techniques, and design strategies before converging on a final design. In addition, these results indicate that the client-based interaction successfully promoted students' curiosity in this module, where students sought clarification, conducted independent research, and questioned assumptions related to scalability, cost, and security effectiveness. The results suggest that embedding design ambiguity within a professional scenario can significantly enhance students' willingness to explore alternatives and justify technical choices.

6.2 Results for Module 2: Network Prototype Development (eKSO 3-c)

The outcome eKSO 3-c for Module 2 examined students' ability to create a network security model that meets client requirements, which perfectly aligns with the EM mindset regarding creating value. This learning outcome focused on application, feasibility, and validation more than a conceptual design.

The result of this outcome is plotted as a pie chart in Figure 2. These results clearly indicate that 67% of students achieved an Excellent level of performance, while 33% achieved an Adequate level, similar to the competency of students observed in Module 1. Similarly, no students fall under the Minimal or Unsatisfactory categories. The results confirm students' success in translating security solutions into working network security prototypes. This consistency between Module 1, for security solutions design, and Module 2, for prototype development outcomes, suggests strong coherence among design, analytical work, and hands-on application.

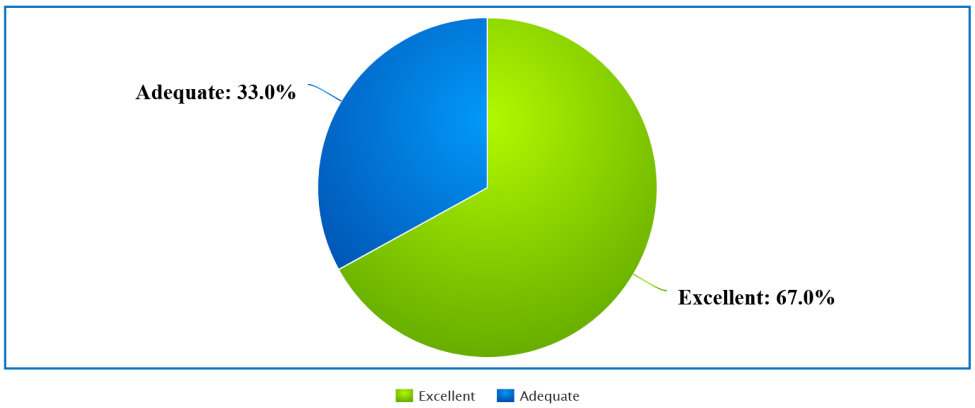

Figure 2: Student Performance in Module 2, eKSO 3-c (Creating Value).

The results of module 2 indicate an important aspect of the EM mindset: value creation requires not only innovative ideas, but also the ability to implement solutions that function under realistic constraints. In short, these results confirm the effectiveness of EML activities in a sequential manner from conceptual exploration to technical realization.

6.3 Results for Module 3: Ethical and Professional Responsibilities (eKSO 6-c)

The third learning outcome eKSO 6-c, for Module 3, studied students' ability to recognize and evaluate potential impacts while making informed ethical and professional decisions. This outcome is directly linked to the EM mindset regarding character.

The data from this outcome is plotted as a pie chart in Figure 3. From Figure 3, the results show that 75% of students achieved an Excellent performance level, while 25% achieved an Adequate level. As in Modules 1 and 2, no students fell into the Minimal or Unsatisfactory categories, which suggests a strong understanding of ethical and professional thinking in network security. The pie chart for this module shows a slightly higher concentration of Excellent performance than in Modules 1 and 2. This result also suggests that students responded more positively to discussions of ethical and professional scenarios when they were linked to real-world responsibilities. In addition, these results confirmed students' ability to evaluate consequences in identifying misuse of access privileges, insider threats, and responsible disclosure.

These results underscore that character development in cybersecurity and network security education benefits organizations with reference to trust, legal compliance, and professional integrity. The strong performance observed suggests that students recognized ethical decision-

making as an integral component of professional cybersecurity practice rather than an abstract theoretical concern.

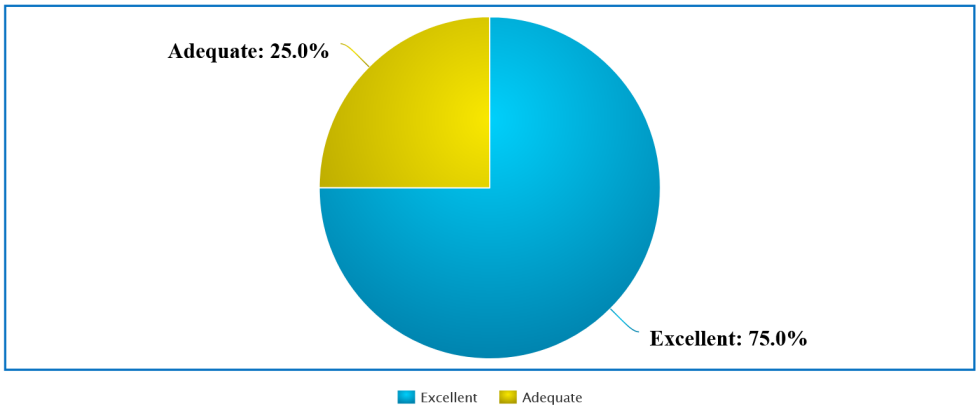

Figure 3: Student Performance in Module 3, eKSO 6-c (Character).

7. Conclusion and Future Work

This paper presents a comprehensive model for integrating the EML into a senior-level Network Security course. In addition, this work demonstrates that the EM mindset can be effectively embedded in a highly technical, hardware-based cybersecurity curriculum. The course modules with EML prepare students to become cybersecurity consultants and solution architects, able to evaluate alternatives, justify design decisions, implement systems, and reflect on the ethical implications of their work. The results confirm that students successfully studied the technical content of the course with EML-based decision-making, stakeholder awareness, and ethical thinking in cybersecurity practice. Thus, educators can cultivate graduates by embedding EML into the network security course, preparing students who are adaptable, reflective, and responsible in the rapidly evolving field of cybersecurity.

This work can be further expanded to include several key areas, such as extending the EML framework to other cybersecurity and networking courses and studying additional aspects of EML for character development. In addition, future offerings of the course will consider inviting industry speakers and mentors to enhance the entrepreneurship mindset and industry engagement.

References

[1] D. Rae and C. Wang, Eds., *Entrepreneurial Learning: New Perspectives in Research, Education and Practice*. New York, NY, USA: Routledge, 2015.

[2] B. H. Sababha, A. Abualbasal, E. Al-Qaralleh, and N. Al-Daher, "Entrepreneurial mindset in engineering education," *Journal of Entrepreneurship Education*, vol. 23, pp. 1–14, 2020.

[3] L. B. Bosman and M. Phillips, "Integrating the entrepreneurial mindset into the engineering classroom," *IEEE Transactions on Education*, vol. 65, no. 2, pp. 150–155, 2021.

[4] M. A. Khan, H. J. LeBlanc, K. S. Al-Olimat, A. Ammar, and F. Jahan, "Incorporating entrepreneurially minded learning (EML) into a computer networks course," in *Proc. ASEE Annual Conf. & Exposition*, Jun. 2025.

[5] N. Rahimi, S. A. Murad, and S. B. Lee, "Entrepreneurship opportunities in cybersecurity," in *Generating Entrepreneurial Ideas With AI*. Hershey, PA, USA: IGI Global, 2024, pp. 172–191.

[6] M. Bishop, *Computer Security: Art and Science*, 2nd ed. Boston, MA, USA: Addison-Wesley Professional, 2018.

[7] M. Hentea, H. S. Dhillon, and M. Dhillon, "Towards changes in information security education," *Journal of Information Technology Education: Research*, vol. 5, no. 1, pp. 221–233, 2006.

[8] T. S. Goetze, "Integrating ethics into computer science education: Multi-, inter-, and transdisciplinary approaches," in *Proc. 54th ACM Tech. Symp. Computer Science Education (SIGCSE)*, vol. 1, Mar. 2023, pp. 645–651.

[9] P. Pusey and W. A. Sadera, "Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference," *Journal of Digital Learning in Teacher Education*, vol. 28, no. 2, pp. 82–85, 2011.

[10] M. A. Khan, H. LeBlanc, K. Al-Olimat, A. Ammar, and F. Jahan, "Incorporating Entrepreneurially Minded Learning (EML) into a Computer Networks Course," ASEE Annual Conference, June 2025

[11] A. Bécue, I. Praça, and J. Gama, "Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities," *Artificial Intelligence Review*, vol. 54, no. 5, pp. 3849–3886, 2021.

[12] K. Dhanushkodi and S. Thejas, "AI enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation," *IEEE Access*, vol. 12, pp. 173127–173136, 2024.

[13] L. O. Nweke, U. F. Okebanama, and G. U. Mba, "Enhancing entrepreneurial skills through experiential learning in IoT, AI, and cybersecurity," *Discover Education*, vol. 4, no. 1, p. 149, 2025.

[14] E. Stavrou and A. Piki, "Cultivating self-efficacy to empower professionals' re-up skilling in cybersecurity," *Information & Computer Security*, vol. 32, no. 4, pp. 523–541, 2024.

[15] KEEN, "The entrepreneurial mindset," Kern Entrepreneurial Engineering Network, 2018. [Online]. Available: https://engineeringunleashed.com/mindset. [Accessed: Jan. 20, 2026].

[16] S. R. Ali, S. Q. Ali, and M. Abbas, "Fostering an entrepreneurial mindset through education: Challenges and opportunities," *Global Social Sciences Review*, vol. 9, no. 4, pp. 179–194, 2025.

[17] R. Banham, "Cybersecurity: A new engagement opportunity," *Journal of Accountancy*, vol. 224, no. 4, p. 28, 2017.

[18] M. Plachkinova and T. Pittz, “Assessing the awareness of cybersecurity within entrepreneurship students: The cyberpreneurship project,” *Entrepreneurship Education and Pedagogy*, vol. 4, no. 3, pp. 564–582, 2021.
[19] S. U. Rehman, “Trends and challenges of project-based learning in computer science and engineering education,” in *Proc. 15th Int. Conf. Education Technology and Computers*, Sep. 2023, pp. 397–403.
[20] M. Antunes, M. Maximiano, and R. Gomes, “A client-centered information security and cybersecurity auditing framework,” *Applied Sciences*, vol. 12, no. 9, p. 4102, 2022.
[21] M. Y. Lee and J. S. Lee, “Project-based learning as a catalyst for integrated STEM education,” *Education Sciences*, vol. 15, no. 7, p. 871, 2025.
[22] F. Naseer, R. Tariq, H. M. Alshahrani, N. Alruwais, and F. N. Al-Wesabi, “Project-based learning framework integrating industry collaboration to enhance student future readiness in higher education,” *Scientific Reports*, vol. 15, no. 1, p. 24985, 2025.
[23] A. T. Sherman *et al.*, “Project-based learning inspires cybersecurity students: A scholarship-for-service research study,” *IEEE Security & Privacy*, vol. 17, no. 3, 2019.
[24] I. Hamburg and K. R. Grosch, “Ethical aspects in cyber security,” *Archives of Business Research*, vol. 5, no. 10, 2017.
[25] M. Christen, B. Gordijn, and M. Loi, *The Ethics of Cybersecurity*. Cham, Switzerland: Springer Nature, 2020.
[26] J. K. Estell, “Embedding the KEEN framework: An assessment plan for measuring ABET student outcomes and entrepreneurial mindset,” in *Proc. ASEE Virtual Annual Conf.*, Jun. 2020.
[27] “Network Security Solution for a Client”, [Online]. Available: https://engineeringunleashed.com/card/edit/2649, [Accessed: 16-Mar-2026].
[28] “Ethical and Professional Responsibilities of a Network Security Specialist”, [Online]. Available: https://engineeringunleashed.com/card/edit/2648, [Accessed: 16-Mar-2026].