Bridging the Gap: Exploring Cybersecurity Careers for High School Students

Gahangir Hossain
Information Science
University of North Texas
Denton, TX, USA
Gahangir.Hossain@unt.edu

Mikyung Shin
Special Education
Illinois State University
Normal, IL, USA
mshin2@ilstu.edu

Mehnaz Afrose
Computer Information Systems
West Texas A&M University
Canyon, USA
mafrose1@buffs.wtamu.edu

Abstract— **This paper aims to present a comprehensive pathway for high school students in grades nine to twelve to pursue careers in cybersecurity. In an era described by way of virtual ubiquity, the paper highlights the vital importance of cybersecurity. It explores the demand for cybersecurity specialists, where there is a significant shortage of skilled professionals, and emphasizes the relevance of cybersecurity in safeguarding online sensitive information. The paper also explores key motivators for high school students, such as the allure of ethical hacking, the opportunity for innovative, hassle-fixing, and the promising profession prospects within the subject. There is a discussion about cybersecurity education for high school students, existing educational initiatives, and programs. This way, the paper presents an overview of various career pathways using cybersecurity career pathway tools. There is a discussion about the obstacles which high school students face on a regular basis in terms of cybersecurity, and some proposals about how to overcome those challenges.**

Keywords— Career Development, Cybersecurity, Education.

The field of cybersecurity has emerged as a critical necessity across government, industries, healthcare, business, academia, and various sectors. However, the shortage of skilled professionals has become increasingly apparent. This study identifies the prospects and considerations surrounding the potential of cybersecurity careers for high school students. The primary goal is to highlight the significance of introducing cybersecurity at the high school level, emphasizing potential challenges, benefits, and the overarching impact on students' academic careers. With a growing demand for cybersecurity expertise in both public and private sectors, there is a critical need for skilled personnel. Consequently, integrating cybersecurity into the high school computing curriculum becomes imperative to align with the future demands of the cybersecurity workforce. This research navigates through basic, intermediate, and advanced modules related to the foundational concepts of cybersecurity curriculum that can be incorporated into high school computing curriculum towards their career in cybersecurity. It includes introducing basic terms and definitions of ethics, security, and privacy concepts, along with best practices in protecting cyber assets. Additionally, hands-on software tools will be proposed for inclusion in the curriculum. Moreover, hands-on projects and real-world application case studies serve as pivotal components, offering students the opportunity to apply theoretical knowledge to practical scenarios. Potential challenges associated with integrating cybersecurity into high school education, such as resource constraints, curriculum adaptation, and teacher preparedness, will also be investigated. Addressing these challenges requires a collaborative effort from educational institutions, policymakers, and industry stakeholders to ensure the effective implementation of cybersecurity education. Furthermore, the research explores the numerous benefits of early exposure to cybersecurity, concluding with a reflection on the long-term impact of introducing cybersecurity education at the high school level. By preparing students with the skills and mindset necessary for success in cybersecurity careers, this research underscores the urgency and importance of embracing future cybersecurity careers.

In this digital era, safeguarding confidential information is becoming crucial as every sector of society, including individuals, government institutions, and private sectors are using cyberspace regular activities [1]. Nowadays, the importance of cybersecurity is paramount [2]. As our lives become increasingly interconnected through digital platforms, safeguarding sensitive information has become critical [3]. Individuals, government institutions, and businesses engage in daily activities within cyberspace, emphasizing the need for robust cybersecurity measures [4]. The pervasive nature of cyber threats underscores the significance of protecting confidential data from malicious actors [5]. In this context, cybersecurity plays a vital role in ensuring the integrity and security of digital ecosystems, reflecting the necessity for effective measures to navigate the complexities of the evolving digital landscape [6].

As the digital age continues to advance, the need for skilled cybersecurity professionals becomes increasingly vital and there is a significant skill gap cybersecurity expertise in each sector and that is creating high-demand career opportunities in cybersecurity for high school and college students [7]. Homework, assignments, and other school students do these days involve computers and the internet along with using these online tools at home for various purposes of curiosity [8]. This paper recognizes the prevalent use of online tools in students' daily lives and aims to bridge the knowledge gap, equipping them with insights into securing their digital presence and fostering a sense of responsibility in the digital realm.

Given the needs of the future workforce in cybersecurity, this paper aimed to enlighten high school students about the stimulating world of cybersecurity and enhance their knowledge about its importance. The intention was to not only impart knowledge but also inspire students to consider a rewarding career path in this high-demand and evolving field. The following research questions guided the current paper:

1. What were the multifaceted aspects and roadmap of cybersecurity career pathways?
2. What machine learning-based methodologies are available to support the decision-making of cybersecurity pathways for high school students?

In essence, the significance of this paper lies in its potential to empower the younger generation with knowledge and skills that are not only relevant to their current academic endeavors but also instrumental in shaping their future career paths. Through exploration and education in cybersecurity, students can not only enhance their digital literacy but also contribute to addressing the critical shortage of cybersecurity experts in the industry [9].

I. Background and Motivation

In the rapidly evolving landscape of information technology, the prevalence and sophistication of cybersecurity threats have reached unprecedented levels [10]. Organizations across the globe face a myriad of challenges as cyber adversaries continue to exploit vulnerabilities for various malicious purposes [11]. Simultaneously, the increasing reliance on digital technologies has propelled the demand for skilled cybersecurity professionals to safeguard critical systems, data, and networks [12]. This overview explores the current state of cybersecurity threats and the escalating need for professionals in this dynamic field.

Navigating the contemporary digital landscape requires a comprehensive understanding of the multifaceted challenges posed by cybersecurity threats [13]. In this intricate domain, Advanced Persistent Threats (APTs) orchestrated by well-funded actors represent a constant menace, seeking to compromise sensitive information, intellectual property, or disrupt critical infrastructure [14]. The alarming surge in ransomware attacks further amplifies the financial and operational risks faced by organizations, as cybercriminals exploit vulnerabilities, encrypt data, and demand ransoms [15]. The persistent use of tactics such as phishing and social engineering underscores the evolving strategies employed by cyber attackers, preying on human vulnerabilities [16]. Moreover, the vulnerabilities embedded on the Internet of Things (IoT) ecosystem expand the attack surface, posing significant risks to critical infrastructure, privacy, and data integrity [17].

These diverse challenges create the need for proactive and vigilant measures to safeguard digital assets in the face of an ever-evolving cybersecurity threat landscape [18]. From targeted APTs to the insidious tactics of ransomware and social engineering, each aspect necessitates a holistic approach to cybersecurity [10]. Recognizing the broader implications of IoT vulnerabilities further emphasizes the interconnected nature of these threats, reinforcing the urgency for comprehensive defense strategies [19]. As the digital realm continues to advance, the role of cybersecurity professionals becomes increasingly pivotal in navigating these complexities and ensuring the resilience of our interconnected world [20].

The importance of cybersecurity knowledge in securing an organization's confidentiality is acknowledged, but in need of the application of this knowledge, the organizations need skilled workforce who are cybersecurity experts [21]. The major obstacle is that there is a workforce deficiency in this sector, which can be approximately 3 million people (about the population of Arkansas) worldwide, according to the cybersecurity workforce studies conducted in 2018 and 2019 [22], [23].

The scarcity of skilled cybersecurity experts is a critical challenge facing industries globally [24]. The evolving nature of cyber threats, coupled with the expanding digital landscape, has led to an increasing demand for adept professionals [25]. Factors such as rapid technological advancements, a lack of standardized career pathways, and the dynamic nature of the field contribute to this shortage [26].

This shortage is further compounded by the absence of a clear and standardized career pathway for individuals entering the cybersecurity field [27]. Unlike some other professions, cybersecurity encompasses a broad spectrum of skills, ranging from ethical hacking and incident response to risk management and compliance [28], [29]. The lack of a well-defined educational and professional development framework makes it challenging for individuals to navigate the field and acquire the specific expertise required by organizations [30].

The consequences of this shortage extend beyond immediate concerns, posing long-term risks to organizations and their ability to defend against evolving cyber threats [31]. To address this challenge, collaborative efforts are essential [32]. Educational institutions, industry stakeholders, and policymakers must work together to establish clear and accessible pathways for individuals interested in cybersecurity [33]. By investing in comprehensive education programs and mentorship initiatives, we can bridge the gap and cultivate a skilled cybersecurity workforce capable of safeguarding our digital infrastructure [34].

This shortage not only highlights the critical need for cybersecurity experts in the industry but also creates a unique opportunity for high school STEM students [35]. With the growing reliance on digital technologies, the demand for cybersecurity professionals is projected to rise steadily in the coming years [36]. Consequently, there exists a window of opportunity for ambitious and tech-savvy high school students to pursue a rewarding career in cybersecurity, filling this workforce gap while contributing to the overall resilience of organizations in the face of evolving cyber threats [37].

In addressing this shortage, high school STEM students can play a pivotal role by equipping themselves with the necessary skills and knowledge to step into the realm of cybersecurity [38]. Initiatives such as specialized cybersecurity programs, workshops, and mentorship opportunities can serve as pathways for these students to develop the expertise sought by organizations worldwide [39]. By fostering a new generation of cybersecurity professionals, we not only mitigate the existing shortage but also ensure a more secure digital landscape for the future [12].

In today's interconnected world, cybersecurity holds paramount importance in our daily lives, influencing how we navigate and interact in the digital landscape [40]. The constant use of online platforms for communication, banking, shopping, and entertainment exposes individuals to various cyber threats [41]. Emphasizing the significance of online safety and data protection becomes essential to safeguard sensitive information [42].

Cybersecurity plays a critical role in protecting personal data from unauthorized access, ensuring the confidentiality and integrity of digital transactions [43]. It extends beyond individual actions, contributing to the overall security of networks, businesses, and governmental organizations [44]. With the increasing frequency of cyberattacks and data breaches, understanding and practicing cybersecurity measures become vital for mitigating risks and maintaining a secure online environment [45].

Educating individuals about the relevance of cybersecurity instills a sense of responsibility for their digital well-being [46]. Implementing strong passwords, being cautious of phishing attempts, and regularly updating software are simple yet effective measures to enhance online safety [47]. The interconnected nature of modern life necessitates a collective effort to prioritize cybersecurity, fostering a secure digital space for everyone [48].

Motivating high school students to explore cybersecurity involves highlighting key aspects that make the field compelling [49]. Ethical hacking, can be seen as a responsible exploration of system vulnerabilities, taps into students' curiosity while fostering a sense of social responsibility [50]. The emphasis on complex problem-solving showcases cybersecurity as an intellectually stimulating domain, encouraging critical thinking skills [51]. Presenting diverse career opportunities within cybersecurity underscores the sustained demand and growth potential in the field [52].

II. Road Map to Cybersecurity Career Pathways

The National Institute of Standards and Technology (NIST) provides many comprehensive resources for professional growth in the cybersecurity sector. The main purpose of these resources is to spell out the diverse array of career pathways accessible within the cybersecurity domain. This section provides some key tools:

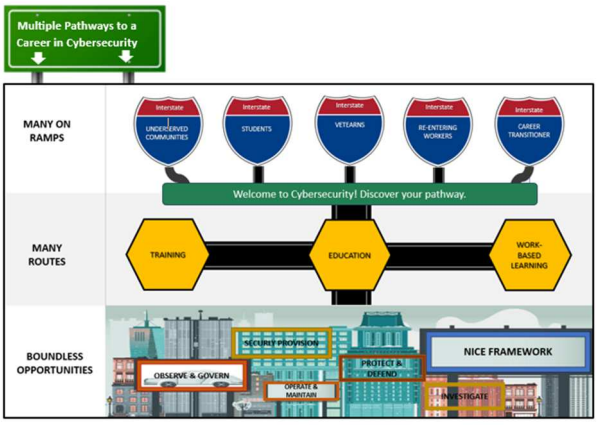

Fig 1. Cybersecurity Career oadmap (figure redrawn from NIST [30])

As depicted in Figure 1, there exist numerous pathways to a career in cybersecurity. Individuals from various backgrounds, including underrepresented communities, veterans, students, those re-entering the workforce, and career transitioners, are all navigating the cybersecurity highway. They have the option to pursue either advanced training to enhance their existing skills (up-skilling) or foundational cybersecurity education with prerequisites such as programming and mathematics to transition into a cybersecurity career (re-skilling) through structured educational programs and hands-on learning experiences. Upon acquiring the necessary cybersecurity education and training, they can pursue their desired roles in a plethora of opportunities, including cybersecurity manager, security specialist, ethical hacker, cloud security specialist, cybersecurity trainer, malware analyst, chief information security officer, and more.

In 2024, a compilation of the top 10 cybersecurity careers along with their average salaries is presented in [53], as illustrated in Figure 2 and summarized in Table 1.

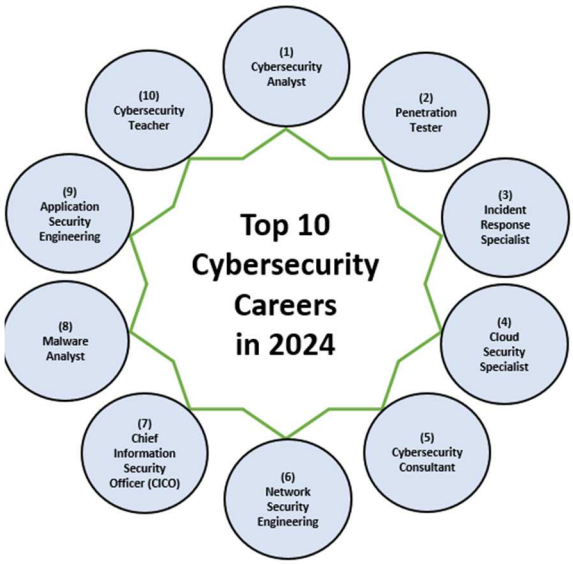

Fig 2. Top 10 Cybersecurity careers in 2024 (figure modified from [53])

TABLE I. Cybercesurity Careers with Responsibilities and Benifits

Job title (with near titles)	Certificates needed	Jobe Responsibilities and Benefits (Average salary as of 2024)
1. Cybersecurity Analyst (or, Security Analyst, Information security Analyst, Security Operation Center Analyst – SOC etc.	Certified Information Security Professional (CISA), CompTIA Security+	The forefront cybersecurity defender safeguards and shields the system. Undertaking analytical duties such as threat detection, incident response, vulnerability assessment, and managing security operations. The annual salary for this position is $110,000.
2.Penetartion Tester (or, ethical hacker, red team analyst)	Certified-Ethical-Hacker (CEH), Offensive-Security-Certified-Professional (OSCP)	Licensed ethical hackers tasked with testing system vulnerabilities, identifying and monitoring weaknesses. Conducting attack simulations, training, and raising awareness among systems and employees regarding system weaknesses. The annual salary for this role is $115,000.
3.Incident Response Specialist (or Incident Responder – Cybersecurity, Incident Handler, Cybersecurity Doctor)	Certified Information Systems Security Professional (CISSP), GIAC - Certified Incident Handling	Forecasting, managing, and mitigating cyber incidents. Addressing security breaches with swift and effective responses, ensuring the fastest possible recovery. The annual salary for this position is $170,000.
4. Cloud Security Specialist (or Cloud Security Engineer, Cloud Security Architect)	Certified Cloud Security Professional (CCSP), AWS Certified Security-Specialist	Concentrating on securing cloud services, environments, and data. Designing and implementing security measures, access controls, and continuously monitoring cloud cyberinfrastructures for potential cyber threats. The annual salary for this role is $70,000.
5. Cybersecurity Consultant (or	Certified Information	Evaluating organizational security and formulating strategic plans for

Security Advisor, Cybersecurity Solution Consultant)	Security Professional (CISSP), Certified Information Security Manager (CISM)	effective defense mechanisms. Conducting cybersecurity risk assessments, developing security policies, implementing countermeasures, and identifying best practices. The annual salary for this position is $115,000.
6. Network Security Engineer (or Network Security Admin, Firewall Engineer)	CISCO certified cybercops associate, Certified network defender (CND)	Concentrating on enhancing organizational cyber infrastructures and network security. Designing and deploying firewalls, VPNs, and monitoring traffic and connections with IPs. The annual salary for this role is $110,000.
7. Chief Information Security Officer (CISO) (or Information Security Director, VP of Cybersecurity)	Certified Information Security Manager (CISM), Certified Information Security Professional (CISSP)	A senior-level cybersecurity professional responsible for strategizing and implementing cybersecurity initiatives across organizations. Aligning with the organization's mission and vision, devising, and overseeing cybersecurity objectives. Providing essential leadership to fortify the organization against cyber threats. The annual salary for this position is $240,000.
8. Malware Analyst (or cyber-threat analyst, malware reverse engineer)	Certified Malware analyst (CMA), Certified Reverse Engineering Analyst (CREA)	Examining malicious software and applications, comprehending their actions, and devising countermeasures. Proficiency in identifying and mitigating emerging cyber threats. Engaging in research on cyber threat operations. The annual salary for this role is $100,000.
9. Application Security Engineer (or software security specialist, application security analyst)	Certified application security engineer (CASE), Certified Ethical Hacker (CEH)	Concentrate on fortifying software application security to thwart vulnerabilities. Execute security assessments, conduct code reviews in collaboration with team members, and strive to intercept breaches at the earliest stages. The compensation for this position is $110,000 per year.
10. Cybersecurity Teacher (or, cybersecurity trainer, Security awareness specialist, cybersecurity training specialist)	CompTIA Security+, Certified Information Systems Security Professional (CISSP)	The responsibilities include crafting, creating, and refining cybersecurity curriculum, courses, and training materials. This entails delivering or facilitating training sessions, assessing performance, and continuously enhancing the training content. The salary for this role is $65,000 annually.

A. Cybersecurity Career pathway tools

Navigating a career path in the ever-evolving field of cybersecurity poses challenges, given the dynamic nature of risks and technologies. Professionals in this industry require strategic guidance and a solid knowledge foundation to progress effectively. To address this need, various tools have been developed to assist individuals in navigating the complex landscape of cybersecurity careers.

These career pathway tools offer valuable insights, recommendations, and tailored roadmaps to accommodate the diverse interests, skills, and objectives of cybersecurity enthusiasts. Whether you're an experienced professional aiming for career advancement or a newcomer eager to explore the vast realm of cybersecurity, these resources provide essential guidance to make informed decisions and pursue your goals with confidence.

Moreover, many of these tools leverage frameworks such as the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, established by institutions like the National Institute of Standards and Technology (NIST), to standardize the classification of cybersecurity roles, tasks, and skills. By adhering to industry-recognized standards and frameworks, these tools enhance their credibility and relevance within the cybersecurity community, ensuring consistency and compatibility across different career trajectories.

1. **CyberSeek**: CyberSeek serves as a comprehensive online platform providing current insights and analysis into the cybersecurity job market landscape across the United States. Offering detailed information on career pathways, sought-after skills, various job roles within cybersecurity, and localized job opportunities, CyberSeek equips users with the tools to navigate the dynamic field of cybersecurity. Through interactive maps and visualizations, CyberSeek empowers individuals to explore the cybersecurity labor market, identify emerging trends, and make informed decisions about their career trajectories. By bridging the gap between job seekers, employers, educators, and policymakers, CyberSeek plays a vital role in supporting workforce development initiatives and addressing the increasing demand for skilled cybersecurity professionals in both public and private sectors.
2. **CyberCareers.gov:** CyberCareers.gov functions as a centralized platform for accessing cybersecurity job openings within the U.S. government. It offers comprehensive details about different positions, eligibility criteria, and application processes within federal agencies, streamlining the recruitment and professional growth processes within the public sector.
3. **My Cyber Path:** My Cyber Path is an extensive online platform designed to assist individuals in navigating the intricacies of cybersecurity employment. Through personalized assessments, skills mapping, and career guidance, it aids users in identifying suitable career paths, acquiring necessary skills, and staying abreast of industry trends. By incorporating frameworks like the NICE Cybersecurity Workforce Framework, it ensures alignment with industry standards. With user-friendly functionalities and data-driven insights, My Cyber Path empowers professionals to make informed decisions and confidently pursue their goals in the rapidly evolving cybersecurity landscape.
4. **Cyber Career Pathways Tool:** The Cyber Career Pathways Tool is a comprehensive resource designed to assist individuals in exploring the diverse array of cybersecurity roles. By leveraging self-assessment tests and personalized recommendations, it helps users identify suitable career paths based on their skills, interests, and goals. Utilizing frameworks like the NICE Cybersecurity Workforce Framework, it categorizes jobs and skills, presenting distinct career trajectories. This tool empowers workers with clarity and confidence, providing insights into industry trends and required qualifications, thereby enabling them to make informed decisions and pursue rewarding careers in cybersecurity.

5. **Dice:** The Dice Tool is an innovative software designed to aid cybersecurity professionals in discovering suitable career paths and opportunities. By employing skill mapping, market analysis, and self-assessment tests, it delivers personalized guidance tailored to individual needs. Leveraging data-driven insights, this tool offers recommendations aligned with user profiles, empowering users to make informed decisions about their career trajectories. Ensuring relevance and consistency, it aligns with industry standards like the NICE Cybersecurity Workforce Framework. With its robust features and user-friendly interface, The Dice Tool equips professionals to navigate the dynamic cybersecurity landscape effectively and accomplish their career goals.
6. **Cyber SN:** CyberSN, a leading cybersecurity talent acquisition platform, offers a specialized tool to aid professionals in exploring job opportunities within the cybersecurity sector. Leveraging advanced algorithms and industry insights, the CyberSN tool matches individuals with suitable positions based on their skills, expertise, and preferences. By optimizing the job search process and delivering personalized recommendations, it enhances efficiency and effectiveness in connecting candidates with employers. Additionally, the tool facilitates professional development through networking events and skill-building opportunities, fostering continuous growth and progression within the cybersecurity field.
7. **Hats & Ladders:** "Hats & Ladders," a dedicated cybersecurity career pathway tool, aims to guide professionals towards career advancement. Through interactive assessments and personalized recommendations, it helps individuals identify their strengths, interests, and areas for improvement. By integrating industry frameworks like the NICE Cybersecurity Workforce Framework, the tool suggests suitable career paths and offers insights into necessary training and certifications. "Hats & Ladders" empowers cybersecurity enthusiasts to make informed decisions and pursue rewarding careers by providing a clear roadmap and tracking progress, bridging the gap between aspirations and achievements in this dynamic industry.
8. **Journeys:** The Journeys Tool is a dynamic application designed to craft tailored career paths in cybersecurity. It assesses individuals' abilities, interests, and aspirations using advanced algorithms and data analytics to offer personalized recommendations for career progression. By leveraging industry standards such as the NICE Cybersecurity Workforce Framework, the tool evaluates users' profiles and delivers customized suggestions for skill development, certifications, and job opportunities. With its user-friendly interface and comprehensive insights, The Journeys Tool empowers cybersecurity professionals to make informed decisions, navigate their career trajectories seamlessly, and stay competitive in the ever-evolving cybersecurity landscape.

III. Making Right Decision to Cybersecurity Career

Numerous cybersecurity career opportunities abound in the market, with reports indicating a scarcity of applicants relative to available positions. Figure 2 and Table 1 collectively illustrate some of the most sought-after cybersecurity roles in 2024 [53]. The question arises: how can a high school student choose the appropriate cybersecurity career? This section outlines a strategic approach using an illustrative decision tree example. When dealing with numerous conditions (features), AI and machine learning strategies can be employed to enhance the decision-making process. Figure 3 shows an example decision tree for a student to choose expected cybersecurity career.

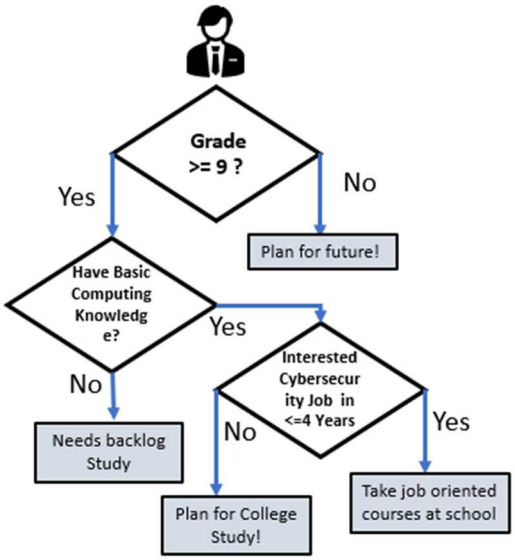

Fig 3. Example -Cybersecurity career decision in 9th grade

A. Decision Tables and Classification

Decision tables serve as a non-procedural specification of decision rules. Their format facilitates systematic documentation of complex business rules. A decision table outlines a logical procedure through a set of conditions and associated actions. Divided into four parts like the table [54], decision tables feature conditions tested and their outcomes. These outcomes typically result in a binary determination (Yes or No, Y/N), or any data value if the decision is multivariate. Based on these outcomes, actions are executed, known as the determination of class level. As depicted in the table [54], X marks denote corresponding class-action entries. Each row in this section of the table is termed an action row.

Example: A student can utilize the following rules to categorize their career choice:

If the student is in 9th grade or higher and possesses basic computing knowledge (understanding of how computers, internet, and cell phones function), classify the student as Type A.

If the student is not in 9th grade but has basic computing knowledge, classify the student as Type B.

If the student is in 9th grade or higher but lacks basic computing knowledge, classify the student as Type C.

If the student is not in 9th grade and lacks basic computing knowledge, classify the student as Type B.

To construct a decision table (see Table II) for the aforementioned scenario, we can identify the conditions and actions specified in each statement. These conditions determine the actions to be taken based on the outcomes of testing the conditions. The relevant condition clauses and action clauses for the problem can be articulated as follows:

RULE 1: If a student is in 9th grade or above (Condition 1) and possesses basic computing knowledge (Condition 2), then classify the career choice as Type A (Action 1).

RULE 2: If a student is below 9th grade (Condition 3) and possesses basic computing knowledge (Condition 2), then classify the career choice as Type B (Action 2).

RULE 3: If a student is in 9th grade or above (Condition 1) and does not have basic computing knowledge (Condition 2), then classify the career choice as Type C (Action 3).

RULE 4: If a student is below 9th grade (Condition 3) and does not have basic computing knowledge (Condition 4), then classify the career choice as Type D (Action 4).

These conditions can be represented as:

Condition 1: Student's Grade >= 9th

Condition 2: Basic Computing Knowledge (BCK) == PASS

Condition 3: Student's Grade < 9th

Condition 4: Basic Computing Knowledge (BCK) == FAIL

TABLE II. DECISION TABLE – CAREER DECISION

	Rule 1	Rule 2	Rule 3	Rule 4
Condition C1: Student's Grade >= 9th	Y	N	Y	N
Condition C2: BCK == PASS	Y	Y	N	N
Action 1: Classify as A	X			
Action 2: Classify as B		X		
Action 3: Classify as C			X	
Action 4: Classify as D				X

We can generate a data table (refer to Table III) including class levels to train a machine learning model. Once the model is trained, it can assist any high school student in making informed career choices within the cybersecurity field.

TABLE III. DECISION TABLE FOR MACHINE LEARNING

	Feature 1 (condition1)	Feature 2 (condition 2)			Feature n (condition n)	Class level
Student#1	1	1				A
Student#2	0	1				B
Studetn#3	1	0				C
Student#4	0	0				D
Student#n	1	0			0	?

As an example, a student (Student #5) with feature vector <1, 0, . . . , 0> can undergo testing using the model.

Considering that high school students' preferences, job-related aptitudes, college readiness, and technology skills are different, learners' diverse characteristics (i.e., features) should be considered in this classification task. Furthermore, academic and other school records across school levels can be used as supporting documentation.

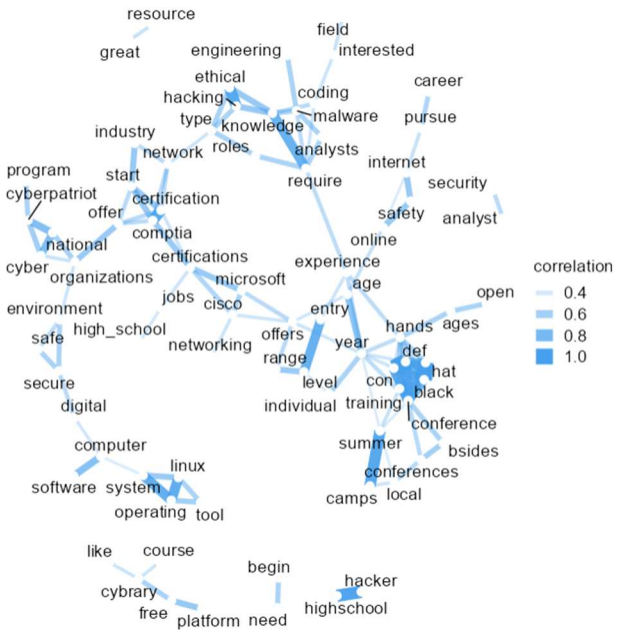

Fig 4. Word network regarding cybersecurity career job descriptions

Figure 4 shows the frequently observed keywords among the career and job descriptions and related resources for high school students [55]. Among words that co-occurred at least four times, keywords such as "system," "Linux," and "operating tool" consisted of a cluster of similar job skills. Additionally, another cluster shows the strong associations among words related to analysts—"malware," "coding," "hacking," "ethical," and "roles"—were also essential elements expected for high school students preparing for their careers in the area of cybersecurity.

This text-mining analysis approach can guide educators and students in quantifying unstructured job descriptions and identifying similar patterns of job-related tasks. With hundreds of resources and descriptions, comprehending all the information could be challenging for many struggling high school learners, including English language learners, dyslexic students, and those with cognitive challenges in information processing and working memories. Meeting their academic and linguistic diversities and needs, these machine learning-based career guidance and automatic summarization of information can be an efficient approach in various education fields. Field-based case studies and the feasibility of these proposed methodologies should be employed and tested across states and countries.

IV. DISCUSSION

The decision-making process for a cybersecurity career is challenging. Within the enormous importance of cybersecurity in everyday life for all people, high school educators, parents, and students inevitably understand the multi-dimensional aspects of various choices after high school graduation. Students should self-evaluate and monitor their plans for their career pathways and successes. Different career choices will require specific certificates and knowledge. In identifying students' cybersecurity careers and guiding decision-making processes, the currently reviewed resources proposed methodologies would provide proactive visions. In providing personalized and data-based pathways, using decision tables and related classifications based on

learners' data can provide valid tools for considering cybersecurity careers. Text mining and detecting word associations from unstructured job descriptions can be another efficient method for students. Future researchers should explore and build public resources together for the community. All the open data and information sharing will validate the decision-making process for high school students and equip them with successful cybersecurity concepts and skills.

V. Limitations and Future Research

Although the researchers proposed cybersecurity career pathways and machine learning-based decision-making methodologies (i.e., decision tree and word following work analysis) for high school students, there are some limitations that guide suggestions for future research. To meet the content validity of cybersecurity career pathways, the team reviewed and proposed methodology based on national technical reports, standards, and protocols (e.g., NICE cybersecurity workforce framework). However, more rigorous review process for the evaluation of cybersecurity pathway tools is needed in the future research. To increase the credibility of the recommended tools, interrater reliability and usability of online resources are recommended. Furthermore, the proposed methodologies should be validated through high school students across various backgrounds and educational needs. Depending on learners' prerequisite background knowledge of STEM and computer science in general, additional support systems should be required in the trajectories. In the future research, researchers can evaluate students' career selection, job-related satisfaction, and job retention rate through a longitudinal study for at least 6 or 8 years to fully assess the effects of the proposed cybersecurity pathways and decision-making approaches.

Acknowledgment

This work has been partially supported by the Office of Naval Research (ONR), USA, Award Number N00014-23-1-2454.

References

[1] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[2] D.-N. Le, R. Kumar, B. K. Mishra, J. M. Chatterjee, and M. Khari, Cyber security in parallel and distributed computing: Concepts, techniques, applications and case studies. John Wiley & Sons, 2019. Accessed: Mar. 26, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=e6iODwAAQBAJ&oi=fnd&pg=PP2&dq=Cyber+security+in+parallel+and+distributed+computing:+Concepts,+techniques,+applications+and+case+studies,+1-37.&ots=Z35tBimYA-&sig=80UXPaA_yMpM64hnY0UAqSA38l8

[3] L. I. Millett, H. S. Lin, and J. Waldo, Engaging privacy and information technology in a digital age. National Academies Press, 2007. Accessed: Mar. 26, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=1qBVAgAAQBAJ&oi=fnd&pg=PT21&dq=3.%09National+Research+Council.+(2007).+Engaging+privacy+and+information+technology+in+a+digital+age.+National+Academies+Press&ots=1qo1YKdJSc&sig=uhw2r2IoEpDQdjFxD5g8845tTXw

[4] F. R. Bechara and S. B. Schuch, "Cybersecurity and global regulatory challenges," Journal of Financial Crime, vol. 28, no. 2, pp. 359–374, 2021.

[5] K. N. Johnson, "Managing cyber risks," Ga. L. Rev., vol. 50, p. 547, 2015.

[6] T. Muhammad, M. T. Munir, M. Z. Munir, and M. W. Zafar, "Integrative Cybersecurity: Merging Zero Trust, Layered Defense, and Global Standards for a Resilient Digital Future," International Journal of Computer Science and Technology, vol. 6, no. 4, pp. 99–135, 2022.

[7] R. Vogel, "Closing the cybersecurity skills gap," Salus Journal, vol. 4, no. 2, pp. 32–46, Nov. 2020, doi: 10.3316/informit.093144667545339.

[8] D. Levin and S. Arafeh, "The digital disconnect: The widening gap between Internet-savvy students and their schools.," 2002, Accessed: Mar. 26, 2024. [Online]. Available: https://eric.ed.gov/?id=ed471133

[9] S. AlDaajeh, H. Saleous, S. Alrabaee, E. Barka, F. Breitinger, and K.-K. Raymond Choo, "The role of national cybersecurity strategies on the improvement of cybersecurity education," Computers & Security, vol. 119, p. 102754, Aug. 2022, doi: 10.1016/j.cose.2022.102754.

[10] O. C. Obi, O. V. Akagha, S. O. Dawodu, A. C. Anyanwu `, S. Onwusinkwue, and I. A. I. Ahmad `, "COMPREHENSIVE REVIEW ON CYBERSECURITY: MODERN THREATS AND ADVANCED DEFENSE STRATEGIES," Computer Science & IT Research Journal, vol. 5, no. 2, Art. no. 2, Feb. 2024, doi: 10.51594/csitrj.v5i2.758.

[11] N. M. Ulsch, Ed., Cyber Threat!, 1st ed. Wiley, 2014. doi: 10.1002/9781118915028.

[12] C. S. Teoh and A. K. Mahmood, "Cybersecurity workforce development for digital economy," The Educational Review, USA, vol. 2, no. 1, pp. 136–146, 2018.

[13] T. VICTOR-MGBACHI, "Navigating Cybersecurity Beyond Compliance: Understanding Your Threat Landscape and Vulnerabilities," 2024, Accessed: Mar. 26, 2024. [Online]. Available: https://www.irejournals.com/formatedpaper/1705360.pdf

[14] S. A. Cohen, "Cybersecurity for Critical Infrastructure: Addressing Threats and Vulnerabilities in Canada," 2019, Accessed: Mar. 26, 2024. [Online]. Available: https://bearworks.missouristate.edu/theses/3340/

[15] L. Y. Connolly and D. S. Wall, "The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures," Computers & Security, vol. 87, p. 101568, 2019.

[16] J. M. Hatfield, "Social engineering in cybersecurity: The evolution of a concept," Computers & Security, vol. 73, pp. 102–113, 2018.

[17] N. Abosata, S. Al-Rubaye, G. Inalhan, and C. Emmanouilidis, "Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications," Sensors, vol. 21, no. 11, p. 3654, 2021.

[18] R. Evren and S. Milson, "The Cyber Threat Landscape: Understanding and Mitigating Risks," EasyChair, 2024. Accessed: Mar. 26, 2024. [Online]. Available: https://easychair.org/publications/preprint_download/sBVG

[19] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2702–2733, 2019.

[20] A. Faizan, "Guardians of the Digital Realm: Navigating the Frontiers of Cybersecurity," Integrated Journal of Science and Technology, vol. 1, no. 2, 2024, Accessed: Mar. 26, 2024. [Online]. Available: https://ijstindex.com/index.php/ijst/article/view/6

[21] B. J. Blažič, "The cybersecurity labour shortage in Europe: Moving to a new concept for education and training," Technology in Society, vol. 67, p. 101769, Nov. 2021, doi: 10.1016/j.techsoc.2021.101769.

[22] R. Ackerman, "Too few cybersecurity professionals is a gigantic problem for 2019," TechCrunch. Accessed: Mar. 26, 2024. [Online]. Available: https://techcrunch.com/2019/01/27/too-few-cybersecurity-professionals-is-a-gigantic-problem-for-2019/

[23] B. Caulkins, T. Marlowe, and A. Reardon, "Cybersecurity Skills to Address Today's Threats," in Advances in Human Factors in Cybersecurity, T. Z. Ahram and D. Nicholson, Eds., Cham: Springer International Publishing, 2019, pp. 187–192. doi: 10.1007/978-3-319-94782-2_18.

[24] K. Ikeda, A. Marshall, and D. Zaharchuk, "Agility, skills and cybersecurity: critical drivers of competitiveness in times of economic uncertainty," Strategy & Leadership, vol. 47, no. 3, pp. 40–48, Jan. 2019, doi: 10.1108/SL-02-2019-0032.

[25] S. Ahmadi, “Next Generation AI-Based Firewalls: A Comparative Study,” International Journal of Computer (IJC), vol. 49, no. 1, pp. 245–262, 2023.

[26] P. Freeman and W. Aspray, “The Supply of Information Technology Workers in the United States,” Computing Research Association, 1100 17th Street, NW, Suite 507, Washington, DC 20036-4632 (Single copy free), 1999. Accessed: Mar. 26, 2024. [Online]. Available: https://eric.ed.gov/?id=ED459346

[27] T. De Zan, “Mitigating the cyber security skills shortage: The influence of national skills competitions on cyber security interest,” http://purl.org/dc/dcmitype/Text, University of Oxford, 2022. Accessed: Mar. 26, 2024. [Online]. Available: https://ora.ox.ac.uk/objects/uuid:916e8d50-7e94-44f0-a8f4-9d496d885a28

[28] E. David, “An Ethical Framework for Cybersecurity Professionals: A Grounded Theory Study,” D.B.A., Northcentral University, United States -- California, 2022. Accessed: Mar. 26, 2024. [Online]. Available: https://www.proquest.com/docview/2746081552/abstract/672514C459104903PQ/1

[29] P. Trim and Y.-I. Lee, Cyber Security Management: A Governance, Risk and Compliance Framework. London: Routledge, 2016. doi: 10.4324/9781315575698.

[30] D. Shoemaker, A. Kohnke, and K. Sigler, A guide to the National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework (2.0). Auerbach Publications, 2018. Accessed: Mar. 26, 2024. [Online].

[31] R. O. Keohane and J. S. Nye, “Power and interdependence,” Survival, vol. 15, no. 4, pp. 158–165, Jul. 1973, doi: 10.1080/00396337308441409.

[32] G. Culot, F. Fattori, M. Podrecca, and M. Sartor, “Addressing industry 4.0 cybersecurity challenges,” IEEE Engineering Management Review, vol. 47, no. 3, pp. 79–86, 2019.

[33] S. N. John, E. Noma-Osaghae, F. Oajide, and K. Okokpujie, “Cybersecurity Education: The Skills Gap, Hurdle!,” in Innovations in Cybersecurity Education, K. Daimi and G. Francia Iii, Eds., Cham: Springer International Publishing, 2020, pp. 361–376. doi: 10.1007/978-3-030-50244-7_18.

[34] L. K. Tsado, “Analysis of cybersecurity threats and vulnerabilities: Skills gap challenges and professional development,” Ph.D., Texas Southern University, United States -- Texas, 2016. Accessed: Mar. 26, 2024. [Online]. Available: https://www.proquest.com/docview/1906329159/abstract/CB1576FBE1734602PQ/1

[35] G. J. Emerick, “Factors that influence students to choose cybersecurity careers: An exploratory study,” Thesis, University of Illinois at Urbana-Champaign, 2020. Accessed: Mar. 26, 2024. [Online]. Available: https://hdl.handle.net/2142/109356

[36] J. Dawson and R. Thomson, “The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance,” Front. Psychol., vol. 9, Jun. 2018, doi: 10.3389/fpsyg.2018.00744.

[37] R. Khanna, Dignity in a digital age: Making tech work for all of us. Simon and Schuster, 2022. Accessed: Mar. 26, 2024. [Online].

[38] S. E. Said, “Pedagogical best practices in higher education national centers of academic excellence/cyber defense centers of academic excellence in cyber defense,” PhD Thesis, Union University, 2018. Accessed: Mar. 26, 2024. [Online]. Available: https://search.proquest.com/openview/cf4fc1b4c2c77a6c0b2cf927ca3ce77f/1?pq-origsite=gscholar&cbl=18750

[39] D. Santos, D. Santos, S. Goel, J. Costanzo, D. Sagen, and P. Buddelmeyer, A roadmap for successful regional alliances and multistakeholder partnerships to build the cybersecurity workforce. US Department of Commerce, National Institute of Standards and Technology …, 2020. Accessed: Mar. 26, 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8287.pdf?utm_source=miragenews&utm_medium=miragenews&utm_campaign=news

[40] N. Al-Hashem and A. Saidi, “The Psychological Aspect of Cybersecurity: Understanding Cyber Threat Perception and Decision-Making,” International Journal of Applied Machine Learning and Computational Intelligence, vol. 13, no. 8, Art. no. 8, Sep. 2023.

[41] H. Saini, Y. S. Rao, and T. C. Panda, “Cyber-crimes and their impacts: A review,” International Journal of Engineering Research and Applications, vol. 2, no. 2, pp. 202–209, 2012.

[42] A. Newman, Protectors of privacy: Regulating personal data in the global economy. Cornell University Press, 2008. Accessed: Mar. 26, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=a2AF8Iji6xUC&oi=fnd&pg=PP13&dq=15.%09Newman,+A.+(2008).+Protectors+of+privacy:+Regulating+personal+data+in+the+global+economy.+Cornell+University+Press.&ots=pLwhhCWVpo&sig=SMBb8PTahkLT-HSVH06k_p3REEo

[43] J. Srinivas, A. K. Das, and N. Kumar, “Government regulations in cyber security: Framework, standards and recommendations,” Future Generation Computer Systems, vol. 92, pp. 178–188, Mar. 2019, doi: 10.1016/j.future.2018.09.063.

[44] A. Dutta and K. McCrohan, “Management’s Role in Information Security in a Cyber Economy,” California Management Review, vol. 45, no. 1, pp. 67–87, Oct. 2002, doi: 10.2307/41166154.

[45] M. F. Safitra, M. Lubis, and H. Fakhrurroja, “Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity,” Sustainability, vol. 15, no. 18, Art. no. 18, Jan. 2023, doi: 10.3390/su151813369.

[46] C. Lewin, D. Niederhauser, Q. Johnson, T. Saito, A. Sakamoto, and R. Sherman, “Safe and responsible internet use in a connected world: Promoting cyber-wellness.,” Canadian Journal of Learning and Technology, vol. 47, no. 4, p. n4, 2021.

[47] S. Purkait, “Phishing counter measures and their effectiveness–literature review,” Information Management & Computer Security, vol. 20, no. 5, pp. 382–420, 2012.

[48] N. Choucri, S. Madnick, and J. Ferwerda, “Institutions for Cyber Security: International Responses and Global Imperatives,” Information Technology for Development, vol. 20, no. 2, pp. 96–121, Apr. 2014, doi: 10.1080/02681102.2013.836699.

[49] L. Zhang-Kennedy, S. Chiasson, and R. Biddle, “The Role of Instructional Design in Persuasion: A Comics Approach for Improving Cybersecurity,” International Journal of Human-Computer Interaction, vol. 32, no. 3, pp. 215–257, Mar. 2016, doi: 10.1080/10447318.2016.1136177.

[50] P. Formosa, M. Wilson, and D. Richards, “A principlist framework for cybersecurity ethics,” Computers & Security, vol. 109, p. 102382, 2021.

[51] S. Nykyporets and V. Chopliak, “Pedagogical strategies for cognitive empowerment: approaches to enhance analytical proficiency in technical university students,” Grail of Science, no. 31, pp. 372–382, 2023.

[52] D. Schuster and S. Wu, “Toward Cyber Workforce Development: An Exploratory Survey of Information Security Professionals,” Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 62, no. 1, pp. 1242–1246, Sep. 2018, doi: 10.1177/1541931218621285.

[53] N. Chaurasia, Top 10 Cybersecurity Career, Top 10 Cybersecurity Careers to Explore in 2024 (sprintzeal.com)

[54] Rajaraman, V. (2011). Analysis and design of information systems. PHI Learning Pvt. Ltd..

[55] Cybersecurity Guide, "How to get started: Cybersecurity for K-12," 2024. [Online]. https://cybersecurityguide.org/resources/k-12-guide.