Evaluation of an Internet of Things Device-Based Educational Approach to Engage a More Diverse Cybersecurity Workforce

6 authors, including:

Maureen Namukasa
Florida Institute of Technology
5 PUBLICATIONS **3** CITATIONS

SEE PROFILE

Maria Chaparro Osman
Florida Institute of Technology
22 PUBLICATIONS **106** CITATIONS

SEE PROFILE

Tj Oconnor
Florida Institute of Technology
36 PUBLICATIONS **438** CITATIONS

SEE PROFILE

Meredith Carroll
Florida Institute of Technology
67 PUBLICATIONS **288** CITATIONS

SEE PROFILE

Evaluation of an Internet of Things Device-Based Educational Approach to Engage a More Diverse Cybersecurity Workforce

Maureen Namukasa, Maria Chaparro Osman, Cherrise Ficke, Isabella Piasecki, TJ OConnor & Meredith Carroll

Published online: 20 Feb 2024.

Submit your article to this journal

View related articles

View Crossmark data

Taylor & Francis
Taylor & Francis Group

Check for updates

Evaluation of an Internet of Things Device-Based Educational Approach to Engage a More Diverse Cybersecurity Workforce

Maureen Namukasa[a] (iD), Maria Chaparro Osman[a], Cherrise Ficke[a], Isabella Piasecki[a], TJ OConnor[b], and Meredith Carroll[a]

[a]College of Aeronautics, Florida Institute of Technology, Melbourne, FL, USA; [b]College of Engineering and Science, Florida Institute of Technology, Melbourne, FL, USA

ABSTRACT

Cybersecurity education heavily utilizes competition-based approaches, such as capture-the-flag (CTF) games to support the need for a skilled cybersecurity workforce. Although CTFs expose students to cybersecurity work competencies, their competitive nature may contribute to the lack of diversity in cybersecurity programs. In response, we developed a technology-based, experiential learning approach utilizing Internet of Things (IoT) devices to educate learners about cybersecurity concepts. We evaluated the approach's effectiveness in engaging and sparking interest in a diverse sample of high school students. Our results indicated that (a) all participants reported a moderate challenge-skill balance, (b) underrepresented minorities (URMs) reported significantly higher engagement than non-URMs, and (c) significantly more female students compared to male students reported increased levels of intent to pursue cybersecurity after participating in the learning activity. We present the approach, methods, results, implications, and recommendations for the use of IoT devices in cybersecurity education to train a more diverse workforce.

1. Introduction

The cybersecurity field has a shortage of professionals despite the increasing demand for these experts and the varying applications of cybersecurity to different sectors of the workplace (Dunn & Merkle, 2018). Moreover, cybersecurity skills are one of the top digital skills required of the future workforce (Li, 2022). The shortage of cybersecurity professionals has been partly attributed to the lack of diversity in the field, with the domain being highly dominated by Caucasian male professionals (Beveridge, 2021; Burrell, 2020; Preston, 2023). Research has shown that gender and ethnic minority disparities were being fostered by the educational and recruitment techniques employed (Riley et al., 2014), which failed to attract and encourage underrepresented minorities (URMs i.e., women, African Americans, and Hispanics) to pursue cybersecurity at an advanced level (Peacock & Irons, 2017). For example, Capture the Flag (CTF) games are commonly used in education settings to teach, engage, and increase student learning outcomes, develop workforce competencies, and deliver enjoyable assessment methods (Leune & Petrilli, 2017). However, CTFs proved effective at recruiting individuals who had already expressed an interest in cybersecurity (Tobey et al., 2014), and the majority of the research was performed with mainly male and or Caucasian participants (Leune & Petrilli, 2017; Ošlejšek et al., 2019). Further, CTFs fail to attract historically marginalized groups, such as females, African Americans, and Hispanic students, who

may not have had previous exposure to the cybersecurity domain (Mountrouidou et al., 2019). Such disadvantaged students are especially affected as CTFs discourage them from entering the security field because they might join the competition feeling inferior to students from better backgrounds (Mirkovic & Peterson, 2014). Examining statistics from CTF competitions revealed that CTFs failed to recruit and engage a diverse cohort of cybersecurity students and professionals. For instance, the 2022 High School Cyber Patriot program and the National Cyber League had approximately 8% African American competitors, and only 25% of the competitors identified as females (Air Force Association, 2022). Further, African American students' interest in the Cyber Patriot program, which attracts youth from all backgrounds, was reported to have deteriorated over the past five years (Air Force Association, 2022), and Hispanic students' representation and success in Advanced Placement (AP) Computer Science was recorded as historically low (Ericson, 2016). The format of CTF competitions may not align with the performance needs of URMs thus rendering CTFs inadequate to stimulate URMs' engagement or provide an ideal challenge-skill balance needed to ignite URM interest and persistence in cybersecurity training. As such, URMs may refrain from the pursuit of, or drop out of, cybersecurity training. This limited URMs' representation in major cybersecurity engagement and instructional platforms provides research gaps for scholars to investigate. It also offers opportunities for instructional designers to

leverage research from multiple disciplines such as learning science, Science Technology Engineering Mathematics (STEM), and instructional approaches to redesign recruitment and training procedures more suited to attract and engage URM students in cybersecurity.

To address this challenge, we proposed a systematic revision of the educational and instructional approaches of future cybersecurity professionals as a crucial step to draw the interest of URMs to the field without stifling non-URMs (e.g., Caucasian, and Asian males) who were already interested. This could help reduce the diversity gap and hopefully meet the ever-increasing demand for professionals in the cybersecurity domain. We designed and evaluated an IoT-based training approach with specific facets to target URMs' situational engagement, optimize their challenge-skill match, and pique URMs' interest and intent to pursue cybersecurity. The goal was to engage a more diverse cybersecurity audience. The approach was grounded in learning science to support its effectiveness and leveraged Internet of Things (IoT) devices to create meaningful and experiential learning opportunities. This manuscript presents a description of the IoT device-based educational approach designed to engage a more diverse cybersecurity workforce, including a presentation of the theoretical and empirical underpinnings of the research, a description of the resulting training module, and the methods, results, and implications associated with an empirical evaluation of the IoT-based approach.

2. Literature review

This section discusses the theoretical foundations and state of science on instructional and engagement strategies from related disciplines that are effective for women and ethnic minorities in learning.

2.1. Applied model of learner engagement

The main foundational theory for the study was the applied model of learner engagement by Carroll et al. (2021). To support learning, Carroll and colleagues proposed that there were three levels of engagement including (1) macro engagement, (2) micro engagement, and (3) flow. Flow is described as a psychological state exemplified by effortless immersion in a task and characterized by enjoyment, increased focus, and feelings of success (Engeser & Rheinberg, 2008; Shernoff et al., 2003) and is the highest level of micro engagement (Carroll et al., 2021). Micro engagement is attained from real-time involvement in an activity, such as participation in a class, whereas macro engagement extends for longer periods such as a learner searching the internet about the material they learned about in the class after the class is over. Carroll et al. (2021) proposed that all three levels of engagement interact with each other and that there are characteristics of the individual, the task, and the environment that influence learner engagement. On the individual level, learner personalities, self-efficacy, interest, and motivation influence engagement. Likewise, facets of the task such as challenge level, goal clarity, feedback, and meaningfulness also influence engagement. Similarly, learner autonomy, safety, and support in the learning environment will also influence engagement. This provided a theoretical foundation to identify interventions that could positively influence learner engagement in cybersecurity instructional materials.

We hypothesized that an educational approach that optimized challenge levels, exemplified abstract material with real-life scenarios to stimulate meaningfulness, and provided a safe and supportive learning environment would be effective at engaging learners in cybersecurity material. All these factors have been reported by extant research to lead to positive learning experiences and engagement. For instance, meaningful learning enhanced comprehension and learning in literature arts, and mathematics (Huang & Chiu, 2015; Mubarok et al., 2022). Further, an optimal challenge and skill fit were reported to contribute to motivation and engagement, and lead to ideal learning experiences among learners (Schneider et al., 2016; Tse et al., 2020), as well as reducing mind wandering and increasing focus on the task among learners (Strandberg-Long, 2021). Additionally, supportive learning environments especially through instructor-student interactions were reported to increase learners' situational and emotional engagement (Chiu, 2021; Lietaert et al., 2015; Pöysä et al., 2019).

2.2. Educating and engaging URMs

There is also empirical work that can be drawn on to understand how to tailor instructional approaches to more effectively engage URMs. Education research has shown that females thrive in collaborative and supportive learning environments versus competitive learning environments (Toda et al., 2019). For instance, the main competitive gamification aspects used in cybersecurity instruction such as CTFs were reported to discourage URMs from pursuing and advancing in cybersecurity education or careers (Jin et al., 2018; Pedro et al., 2015; Zahedi et al., 2021). This is partly because females are more interested in the social aspects of cybersecurity rather than individual competition against each other (Rowland, 2018; Toda et al., 2019). Further, females have shown a preference for learning environments that foster social cooperation rather than competition (Toda et al., 2019). Although gamification is widely used for cyber competitions like CTFs, and supports overall learner engagement, most competitive traits of gamification such as leaderboards and virtual points are not perceived as motivating or enjoyable for females (Jin et al., 2018; Zahedi et al., 2021). Rather, females thrive where there is collaboration and support from the learning environments (Sax et al., 2017) and show more interest and enjoyment when there is less pressure from the learning environment (Pedro et al., 2015). Moreover, social-cultural learning theories support that females' perceptions of the learning environment can be crucial in influencing their career decisions such that they are likely to drop out of careers for which they have a negative perception of the learning environment (Balakrishnan & Low, 2016; Hosaka, 2014).

Similar findings were reported for ethnic minorities, for instance, collaborating in teams and acknowledging the contribution of team members created interest and motivation for African Americans in cyber-related areas by increasing their self-efficacy and interest in Science and Engineering fields (Kornegay et al., 2021; Rockinson-Szapkiw et al., 2021). Besides social learning environments, early exposure of URMs to cybersecurity material and concepts has also been argued to be a significant factor in increasing familiarity with cybersecurity concepts. For example, early exposure developed interest among URMs in the cybersecurity field and enhanced persistence in Computer Science in college (Hurtado et al., 2009; Lingelbach, 2018; Malecki, 2018; Sax et al., 2017; Weston et al., 2020). Further, proponents of the expectancy-value theory of achievement motivation posit that individuals decide which activities to pursue based on their ability beliefs (Wigfield & Eccles, 2000). Hence, for girls and boys, these ability beliefs are fostered by stereotypes (Eccles et al., 1993). For instance, biases that may have developed about a certain activity can either encourage or deter girls or boys from participating in the activity. Research has also shown that the misconception that cybersecurity is associated with males was one of the roadblocks that deterred women's advancement in the field (Cheryan et al., 2015; Pinchot et al., 2020; Sax et al., 2017). To level the playing field, a revision of how such subjects are presented needs restructuring to debunk any stereotypes individuals may have developed about cybersecurity professionals. Further, proponents of the social practice theory have argued that the underrepresentation of women of color in STEM was explained by the issue of identity. For instance, many African-American women who excelled in Science subjects did not pursue STEM careers because they did not identify with the Science community (Kang et al., 2019). This is further expounded by the issue of representation in cybersecurity. Scholars concur that many minorities do not thrive or advance in Computer Science-related areas because of the lack of representation of others (such as women, African Americans, and Hispanics) with whom they identify (Cherry et al., 2020; Shumba et al., 2013; White et al., 2018). To engage and educate URMs in cybersecurity, there are many aspects of the instruction that require intervention to ignite their interest and yield engagement in domains to which they are not historically attracted. Such aspects may include facets of the task (e.g., collaboration, challenge-skill match, experiential learning), the learning environment (e.g., instructor support, collaboration, scaffolding), and how learning materials are presented to these URMs.

2.3. Instructional and engagement strategies

Based on our recent study by Osman et al. (2023) and a review of other extant literature, there are several strategies shown to be effective at engaging and educating URM students about cybersecurity and other STEM fields (Daud, 2022; Gray & Ross, 2020; Jethwani et al., 2017; Jin et al., 2021; Kornegay et al., 2021; White et al., 2018). Seven strategies were selected for inclusion in our IoT-based training approach to engage URMs in cybersecurity. These instructional and engagement strategies, which are expanded upon below, include (a) problem-based learning, (b) scaffolding, (c) collaborative learning, (d) experiential learning, (e) gamification, (f) challenge/skill match, and (g) representation.

2.3.1. Problem-based learning
Problem-based learning is an instructional strategy that challenges learners to think, create, and test possible solutions (Walker et al., 2015). Extant research suggests that an emphasis on creative and collaborative problem-solving processes in cybersecurity is likely to increase girls' engagement in the field (Jethwani et al., 2017). Further, the significance and deficiency of problem-solving skills among cyber professionals and graduates was noted by several scholars (Arora, 2019; Hoyne et al., 2016; Nygard et al., 2018; Wahsheh & Mekonnen, 2019; Walker et al., 2015).

2.3.2. Scaffolding
The concept of scaffolding stems from a combination of the Zone of Proximal Development and sociocultural aspects (Verenikina, 2003) and is described as the process of providing support, hints, and prompts to the learner that fade away as the learner's knowledge and skills increase (Carroll et al., 2021). The benefits of scaffolding include the transfer of knowledge, motivation (Schmidt et al., 2011; Simons & Klein, 2007), and improved perception of learners' challenge/skill balance (Belland et al., 2013). Further, a heavily teacher-supported scaffolding technique was found to be more effective at teaching girls computational thinking and developing their self-efficacy compared to a limited teacher-supported scaffolding method (Jin et al., 2021).

2.3.3. Collaborative learning
Collaborative learning is a form of social learning that involves two or more learners working collectively toward a task to achieve a common goal in learning (Laal & Laal, 2012). It can be exemplified in classroom environments when learners are tasked to complete assignments in teams (Chounta, 2020; Dillenbourg, 1999). Females prefer learning in collaborative environments (Reychav & McHaney, 2017; Sax et al., 2017), and collaborative learning has been linked to increased motivation for African-American learners in cybersecurity-related areas (Kornegay et al., 2021).

2.3.4. Experiential learning
Experiential learning is a pedagogical tool that includes activities that allow active involvement of the learners or hands-on learning and critical thinking about the material being taught (Bradberry & De Maio, 2019; Carlson & Maxa, 1998). Hands-on learning tools such as labs, simulations, and projects can be used to teach cybersecurity content by providing students the ability to use, practice, and apply learned skills. These experiential learning tools can lead to

higher engagement and knowledge retention (Johnson et al., 2021; Stull & Mayer, 2007). In cybersecurity, experiential learning has been found to increase self-efficacy and cybersecurity knowledge among high school students (Konak, 2018). Further, experiential learning benefits were profound for students of color (Daud, 2022) and females (Gray & Ross, 2020) in technology instruction and geometry respectively.

2.3.5. Gamification

Gamification is described as using game design and associated elements to transform non-game contexts (Deterding et al., 2011; Werbach & Hunter, 2015). Research in learning shows that gamification improves learner outcomes (Hamari et al., 2014), such as increasing the number of completed assignments (Laskowski & Badurowicz, 2014) and increasing learner motivation (Zahedi et al., 2021). However, some aspects of gamification that focus on individual competition versus collaboration have been shown to have negative outcomes, and lead to demotivation for females (Pedro et al., 2015; Zahedi et al., 2021), and tend to attract participants who already have experience with cybersecurity (Tobey et al., 2014). Therefore, layering gamification features such as personal leaderboards, badges, and social competition that led to engagement in all students without demotivating URM groups (Iosup & Epema, 2014; Zahedi et al., 2021) may prove beneficial.

2.3.6. Challenge-Skill match

Challenge-skill match is a characteristic of the flow experience that can be attained when there is a perceived optimization between the perceived difficulty of a task and the perceived skill of an individual (Engeser & Rheinberg, 2008; Shernoff et al., 2003) leading to enhanced student learning outcomes (Shernoff, 2013). Flow is attained from active involvement in a task and is typically associated with high levels of engagement (Carroll et al., 2021; Shernoff & Anderson, 2014; Shernoff & Csikszentmihalyi, 2009; Whitson & Consoli, 2009). Individuals attain the flow state when the task demands are not too low to cause boredom nor too challenging to cause frustration (Bloom, 1976; Csikszentmihalyi, 2014). Research has found that perceived challenge and skill have a positive relationship with learning (Hamari et al., 2016), is an important facet of overall engagement (Hamari & Koivisto, 2014; Procci et al., 2012; Wang & Chen, 2010), and when balanced can yield high levels of intrinsic motivation for students (Renninger & Hidi, 2015).

2.3.7. Representation

Representation involves the presence of minorities, including women, African Americans, and Hispanics, in the cybersecurity industry, faculty, and the student body (Esin, 2020). Studies have shown that underrepresented minorities find inspiration, motivation, and encouragement from the success stories of role models who look like them (Cobb, 2018;

Kricorian et al., 2020; Pietri et al., 2021; Rowland, 2018). However, the lack of representation is a consistent factor that has hindered URMs' professional development in Computer Science (Cherry et al., 2020; Shumba et al., 2013; White et al., 2018).

2.3.8. IoT devices for learner engagement

The second approach to address this gap was the utilization of IoT devices to teach and engage the younger generation of students about cybersecurity concepts. IoT devices are everyday devices, such as smart thermostats, smart fridges, and smart doorbells that can be controlled by a smartphone or computer through remote access. IoT devices can create meaningful learning experiences for students of all calibers because of their ubiquity. Further, as the majority of learners are familiar with IoT devices, the gadgets provide equal learning opportunities and foster the understanding of abstract concepts such as networks, reverse engineering, and cryptography. IoT devices also offer hands-on opportunities for learning that stimulate situational engagement in trained material. Using familiar technology makes the concepts realistic, relatable, and meaningful. Moreover, IoT devices are affordable, which increases their accessibility to disadvantaged students unlike pricey games typically used in CTFs to which such students may not have access (Mirkovic & Peterson, 2014). IoT has diverse applications such as smart cities, utilities, buildings, and appliances (Fernández-Caramés & Fraga-Lamas, 2020; Tariq et al., 2023), hence making IoT an ideal teaching tool for topics such as security, privacy, networking, wireless sensors, localization, and routing (Burd et al., 2018).

Implementation of education utilizing IoT has been considered an ideal approach for the modification and transformation of the education environment with utility for both teachers and students (Abdel-Basset et al., 2019). Some scholars have used IoT devices to teach students about technological content in which students' prior knowledge was low (Chothia & De Ruiter, 2016; Mäenpää et al., 2015). Others have focused on IoT security, for example, Chothia and De Ruiter (2016) utilized IoT devices in the classroom to teach cybersecurity concepts and found that the low level of IoT device security lends itself well to cybersecurity education because basic vulnerabilities are easy to find with these devices without a requirement for advanced security skills or training. IoT devices have also been reported to support authentic and real-world applications and retention of learned material (Ban et al., 2017; Giannakas et al., 2022). A study by Giannakas et al. (2022) evaluated aspects of learning including learning effectiveness, efficiency, knowledge acquisition, and learner satisfaction using a blended IoT device-based curriculum to teach students about encryption and decryption techniques. Results indicated a highly effective and efficient strategy, above 50% satisfaction, and improved knowledge acquisition among participants. IoT devices offer an opportunity to master the taxonomy of cybersecurity workforce competencies including embedded systems programming, data gathering, storage, system

vulnerability, analysis, and cloud and web technologies. Hence, the use of an IoT device provides a great foundational instructional tool that facilitates the layering of instructional strategies aimed at engaging and training URM students in cybersecurity. Despite the utility of IoT platforms in cybersecurity training, limited research has endeavored to empirically investigate the impact of such training platforms on learner engagement and interest in cybersecurity, specifically with URMs. As such, this effort aimed to build upon our recent qualitative work on the diversification of the cybersecurity workforce (see Osman et al., 2023) by empirically evaluating an instructional approach. The goals of the evaluation were to determine the feasibility of implementing an IoT-based educational approach with a diverse high school sample and to evaluate the impact the approach had on learner engagement and intent to pursue cybersecurity with a special focus on URM students.

3. Methods

3.1. Educational approach

The following section describes the approach that was used to design an instructional module to promote URMs' engagement in cybersecurity instruction and the resulting module. It also expands on how the instructional strategies shown to be effective with URMs were blended with an IoT device as the primary hardware platform. It is organized as follows: (a) module overview, (b) IoT platform description, and (c) module description.

3.1.1. Module overview

The module was developed for high school students with minimal experience with, and skills in, cybersecurity. The module's learning objectives were based on the National Institute of Standards and Technology (NIST) Knowledge Skills and Abilities (KSA). We identified and introduced the topic of Network Traffic Analysis by leveraging an IoT device in the form of a remote-control (RC) car, in conjunction with Wireshark protocol analyzer software to allow the students to investigate previously captured car traffic. Network traffic analysis is a fundamental skill required by cyber defense analysts, incident responders, and information systems security managers (Petersen et al., 2020). An analyst may review network traffic in a workforce role to determine the source of a compromise to the system or determine if an attacker has stolen proprietary information. This module introduced practical adversarial thinking by challenging students to analyze traffic and reverse engineer the IP address, port, password, and commands necessary to control a car remotely.

3.1.2. IoT platform description

We determined that a RC car (see Figure 1) was an ideal IoT device platform for teaching the Network Traffic Analysis module because it can allow K-12 faculty to easily reproduce activities and scale them for a broader impact in

Figure 1. The RC car platform.

a cost-effective manner. Further, we pilot-tested the RC cars extensively with diverse groups (e.g., attendees at cybersecurity conferences, both less technical and non-technical college-level students in laboratory settings) to ensure ease of use, and ability to ignite situational engagement. The car model was a LABISTS Raspberry Pi Smart Car and was powered by a rechargeable lithium battery, controlled using a Raspberry Pi computer running a custom service on a wireless network. We ran the Wireshark application on laptop computers to enable students to read previously captured network packets of the RC cars. We also added the Netcat application to laptop computers for learners to use as a working terminal to support interaction with, and control of, the RC cars by running commands within it. As described in the following section, the students were able to analyze network traffic using the Wireshark application and connect to the car by running commands in the Netcat application. The use of an RC car and Raspberry Pi computer allowed for the replication of the activity cost-effectively.

3.1.3. Module description

The module was entitled, King of the Packet: Forensically Analyzing Network Traffic, which was delivered using a combination of PowerPoint slides, remote control cars, Wireshark, and Netcat tools. The module was conducted in four chronological segments: (a) attention hook, (b) background lecture, (c) guided instruction, and (d) hands-on activity. Further, to engage the students, URMs in particular, the instructional and engagement strategies discussed above were layered throughout these sections of the module as described below. This evaluation was a preliminary study of one module as part of an 8-module curriculum being developed for a longitudinal evaluation of instructional strategies and IoT-based curricula targeting women and minorities in cybersecurity education. The results were used to help inform the design of other modules within the curriculum. The following paragraphs describe the four segments of the module.

First, we used an attention hook to capture the learners' attention and stimulate meaningfulness to the learners by presenting a real-life security scenario that involved a

United States military drone crash in enemy territory that resulted in an enemy takeover. We then challenged learners to identify the skills the enemies utilized to crash and take over the drone. Next, we discussed the technical terms of spoofing and jamming attacks that the enemies used to compromise the Global Positioning System (GPS), telemetry, and video feeds of the drone. This was also the first step in implementing problem-based learning and collaborative learning because learners were tasked to work in teams, to determine how enemies managed to hack the drone and crash it in enemy territory in a scenario-based discussion format. Once the allocated time for group discussions had elapsed, a representative from the team of learners was asked to articulate the team's answers to the instructor.

Second, we presented a brief slide-based background lecture introducing terminology and network security subject matter including communication protocols such as transmission control protocol (TCP) traffic, and user datagram protocol (UDP) traffic, networks, and addresses. Further, images of network packets and their interpretation, and the Wireshark toolkit, which is software that opens the network packets, were presented to familiarize learners with the software platform that they would be interacting with during the hands-on activities.

Third, a guided instruction session ensued during which each learner team was assigned a researcher to guide learner teams through the process of analysis, and provide support, hints, and prompts when necessary. Teams were tasked to investigate previously recorded network packets to identify patterns and meanings behind the network patterns, to figure out previously used commands (e.g., turn left, forward, turn right, and turn on lights), and to obtain control of the RC cars assigned to each team. The guided instruction utilized an experiential learning format by allowing the learners to work through the challenges, hands-on, by interacting with both the RC car and the software applications controlling the car remotely. Scaffolding was utilized by embedding a researcher within each team to deliver guidance and a series of prompts, as needed, which urged learners in the right direction, and encouraged as learners progressed through the activity. As learners' skills increased during the session, the researcher would reduce the assistance accordingly. Further, the strategy of representation was achieved by ensuring the 9-person research team assisting the learners was comprised of URMs including six women, of which one was Black, and two were Hispanic.

Finally, the teams competed in a *King of the Hill* game during which they worked collaboratively to utilize the interface they had been interacting with, to drive their cars from a predefined starting point to a centrally located traffic cone, and maintain contact with the traffic cone for at least two minutes. During the game, prompting was utilized to manage the level of challenge and match it to each group's competence. Through researcher support, learners applied problem-solving techniques and discovered that they could control the fate of the game by using learned skills to hack into other teams' cars, obtain control of the cars, and drive them away from the target. Teams could only connect to a single car at a time because each car was connected to a separate wireless network. Thus, a team that attacked another team's car was forced to abandon control of their own car for that period. This created a very dynamic and engaging gamified environment by having the teams compete against each other for a candy reward.

3.2. Evaluation

This section presents the procedures used to evaluate the effectiveness of the module, and the resulting findings and implications. The King of the Packet module was evaluated with two local high schools in Southeastern Florida. The goals of the evaluation were to determine the feasibility of implementing the lesson with a diverse high school population and to evaluate the impact the approach had on learner engagement and intent to pursue cybersecurity, for URMs in particular.

3.2.1. Participants
Participants were recruited through their respective high schools' Junior Reserve Officers Training Corps (JROTC) programs. The schools were selected based on convenience sampling due to school proximity and professional contacts within the high school administrations. A total of 34 junior- and senior-level high school students participated in the study. However, the final sample included in the data analysis was $N = 30$ participants due to the exclusion of four participants who lacked parental consent forms. Six participants did not complete all relevant survey questions and were therefore excluded from individual analyses in which they had missing data.

The average age of the participants, $N = 30$ was 17.23 years ($SD = 1.17$) ranging from 15 to 19 years old. Of these, 20 were URMs which included females, African Americans, and Hispanics, whereas 10 were non-URMs which included Caucasian and Asian males. Eighty-three percent of the participants were proficient in English and, 17% reported speaking English relatively well. Fifty percent of the participants had no previous Computer Science experience, 47% had some experience with Computer Science, and 3% understood coding and had knowledge of a programming language. All other demographic data are summarized in Table 1. The study was approved by the Florida Institute of Technology Institutional Review Board.

3.2.2. Experimental design
The study was a within-groups repeated measures design with all the participants experiencing the same treatment: exposure to an introductory cybersecurity lesson on network traffic analysis with an integrated hands-on activity as described above. Pre-tests and post-tests were administered to determine the influence that the lesson had on participants' intent to pursue cybersecurity. Post-tests were administered to evaluate the challenge-skill match for high school students and learner engagement levels. Between groups independent variables of URM status (URM vs. non-URM)

Table 1. Demographic information.

Variable	n	%
Age		
≥17	13	43
≤18	17	57
Biological Sex		
Male	16	53
Female	14	47
Ethnicity[a]		
Hispanic/Latino	5	17
Not Hispanic	20	69
Race[b]		
African American/ Black	8	27
Asian	3	10
Caucasian	14	47
English first language		
Yes	26	87
No	4	13
Cybersecurity Experience		
No experience	22	73
Less than 1 year	6	20
1 year or more	2	7

Note. $N = 30$.
[a] 4 participants selected "other" under ethnicity.
[b] 5 participants selected "other" under race.

and biological sex at birth (Male vs. Female) were also examined post hoc.

3.2.3. Measures

The following measures were captured during the evaluation.

3.2.3.1. Demographics. Pre-surveys were administered to collect individual difference data including, (a) age, (b) biological sex (male, female, and prefer not to say), (c) race (African American, Asian, Caucasian, and other), (d) ethnicity (Hispanic, not Hispanic, and other), (e) Computer Science experience (no prior experience, some experience with coding, understand coding, and other), (f) English as first language (yes and no), English proficiency (very well, well, not well, and not at all), and (g) cybersecurity experience (no experience, less than a year, one year to less than three years, three years to less than five years, and other).

3.2.3.2. Challenge-skill match. An important aspect of engagement is challenge-skill match, which is the balance between the perceived difficulty of the task and the perceived skill of the individual involved in the tasks (Engeser & Rheinberg, 2008). A challenge-skill measure helped to determine the appropriateness of the module for an introductory-level cybersecurity program for high school students, and especially URMs. Challenge-skill match was measured using the 3-item challenge/skill match subscale on the Flow Short Scale (FSS; Rheinberg et al., 2003). These items were administered in a post-survey and measured the perceived difficulty of the task, perceived skill, and perceived fit of difficulty and skill on a 9-point scale.

3.2.3.3. Engagement. The absorption subscale of the FSS was utilized in the post-survey to examine learner engagement in the learning activity. Flow represents a type of engagement

that focuses on concentration and involvement in a task or activity (Delle Fave, 2013). The FSS is a 13-item questionnaire that measures Flow Experience using two components: fluency of performance and absorption by activity (using the first 10 items) and perceived importance (using the last 3 items). The items are measured on a 7-point scale.

3.2.3.4. Intent to pursue cybersecurity. Participants' future interest in cybersecurity was examined by gauging their intent to pursue an advanced cybersecurity education or career. This was assessed using a researcher-developed item administered both in the pre-survey before exposure to the lesson and in the post-survey after exposing them to the lesson. The intent item asked, "Are you interested in pursuing a cybersecurity profession/degree?" and was measured on a scale of four including (1) I have no intention of pursuing a cybersecurity education or career, (2) I might consider pursuing a cybersecurity education or career, (3) I am considering pursuing a cybersecurity education or career, and (4) I intend to pursue a cybersecurity education or career. To determine if there was a change in participants' interest in cybersecurity, a difference was computed between their pre-test and post-test scores.

3.2.3.5. Learner reactions to the lesson/activity. Researcher-developed open-ended questions were included in the post-survey to obtain qualitative participant reactions to the lesson. The questions examined what the learners specifically enjoyed and disliked about the lesson and activity. All data were collected using Qualtrics survey software.

3.2.4. Procedures

Due to participants being under the age of 18, prior to the day of the evaluation, parental consent forms and student assent forms were sent to the local high schools for review and signature. Before beginning the evaluation, the researchers obtained the signed consent forms and developed a list of students who did not have parental consent. Although these students were interested and allowed to participate, we ensured that their data were excluded from the analyses.

Participants first completed pre-surveys on electronic tablets and were then divided into teams of four or five with an emphasis on diversity within each team with respect to biological sex, ethnicity, race, and computer science experience. Each team was assigned at least one researcher to support the team throughout the module's activities.

The module was then delivered per the description in the previous section and lasted approximately 45 minutes. During the activity, each team received varying levels of support from researchers, based on their skill level, to ensure teams made sufficient progress during guided instruction and were able to compete at adequate levels in the activity.

Teams then competed against each other in the activity until the allocated time for the activity was used up, and the winning team was announced. All participants received a candy reward and then completed post-surveys on electronic

tablets. The full evaluation was concluded in approximately 60 minutes.

4. Results

The data were analyzed using Statistical Package for Social Sciences (SPSS V. 26). As the study was an ex-post facto approach, once the data were collected, it was coded accordingly to identify learners who were defined as URMs in cybersecurity, including women, Hispanics, and African Americans. Those who were not considered URMs in cybersecurity (e.g., Caucasian, and Asian males) were coded as non-URMs. Once the two main groups were identified from the dataset, analyses were conducted. Descriptive and inferential statistics including, independent t-tests, Chi-square analyses, and Multivariate Analyses of Variance (MANOVA) were conducted to determine any statistical significance in the different dependent variables between URMs (females, African Americans, and Hispanics) and non-URMS (Caucasian and Asian males) and between males and females. The following section expands on the findings of the study.

4.1. Challenge-skill match

The mean level of difficulty experienced by participants, $N = 23$ on a 9-point scale from easy to difficult was moderate ($M = 5.22$, $SD = 1.41$), perceived skills related to the material that was taught on a 9-point scale from high to low, were moderate ($M = 5.43$, $SD = 1.38$), and the perceived balance on a 9-point scale from too high to too low, was moderate ($M = 5.04$, $SD = .77$). Thus, overall, participants did not find the lesson or activity too challenging. The results were further examined at the group level to determine if there were any differences in challenge-skill match experienced between groups. To determine if URMs and non-URMs or males and females reported differences in the perceived challenge-skill match about the lesson and activity, a MANOVA was conducted with minority grouping as the independent variable at two levels (URMS vs. non-URMs) and difficulty, perceived skills, and perceived balance as the dependent variables. The omnibus test revealed that the main effect of URM and non-URM on challenge-skill match was not significant, $F(3, 19) = 1.28$, $p = .31$). The groups were then examined using MANOVA with biological sex as the independent variable at two levels (males vs. females) and difficulty, perceived skill, and perceived balance as the dependent variables. The omnibus test of the main effect of biological sex on challenge-skill match was also not significant, $F(3, 19) = .37$, $p = .78$).

4.2. Learner engagement

When examining learner engagement, the average engagement experienced by participants, $N = 24$ on a 7-point scale was high, $M = 5.21$, $SD = .79$. The results were further examined at the group level. When examined at the minority group level, URMs ($M = 5.4$, $SD = .74$) reported higher engagement than non-URMs ($M = 4.9$, $SD = .81$). An independent samples t-test was conducted to determine whether the differences in engagement experienced between these groups were significant with minority grouping as the independent variable at two levels (URM vs. non-URMS) and engagement as the dependent variable. Results revealed that the difference in engagement experienced between URMs and non-URMs was significant, $t(22) = 1.72$, $p = .05$, $d = .727$, suggesting that differences in levels of engagement experienced between URM and non-URM participants varied significantly. When comparing the results by biological sex, males ($M = 4.9$, $SD = .77$) yielded lower engagement compared to females ($M = 5.5$, $SD = .71$). To determine if the difference in engagement by biological sex was significant, an independent samples t-test was computed with biological sex as the independent variable at two levels (males vs. females) and engagement as the dependent variable. The results were significant, $t(22) = 2.03$, $p = .027$, $d = .833$, suggesting that females found the activity more engaging than males. See Figure 2 for a graphical representation of engagement experienced by groups.

4.3. Intent to pursue cybersecurity

The change in the intent to pursue cybersecurity from the pretest to the posttest was compared between URMs and non-URMs, and males versus females, to determine whether there were any trends in a change in intent to pursue cybersecurity. Out of the 18 URMs, 13 had no change in intent, four had an increase in intent, and one had a decrease. On the other hand, out of the 10 non-URMs, nine had no change in intent and one had a decrease. Overall, more URMs (46.43%) reported no change in intent compared to non-URMs (32.14%), only URMs reported an increase in intent (14.28%), and at least one participant reported a decrease in intent to pursue in both URM and non-URM groups. These trends in intent change were then analyzed using the Chi-Square test of independence. The results revealed that there was no significant difference in the change in intent to pursue cybersecurity between URMs and non-URMs, $X^2(2, N = 28) = 2.66$, $p = .27$.

When examining biological sex, results revealed that out of 16 males, 15 reported no change and one reported a decrease in intent to pursue cybersecurity. However, out of the 12 females, four reported an increase in intent to pursue, seven reported no change, and one reported a decrease in intent to pursue cybersecurity. Overall, more males (53.57%) reported no change in intent compared to females (25%), and only females (14.28%) reported an increase in intent to pursue cybersecurity. At least one male and one female participant reported a decrease in intent. These trends were analyzed using a Chi-Square test of independence and results revealed that the relationship between the increase in intent and biological sex was significant $X^2(2, N = 28) = 6.47$, $p = .039$, suggesting that females were more likely to yield an increase in intent to pursue cybersecurity compared to males after exposure to the cybersecurity lesson (see Figure 3).
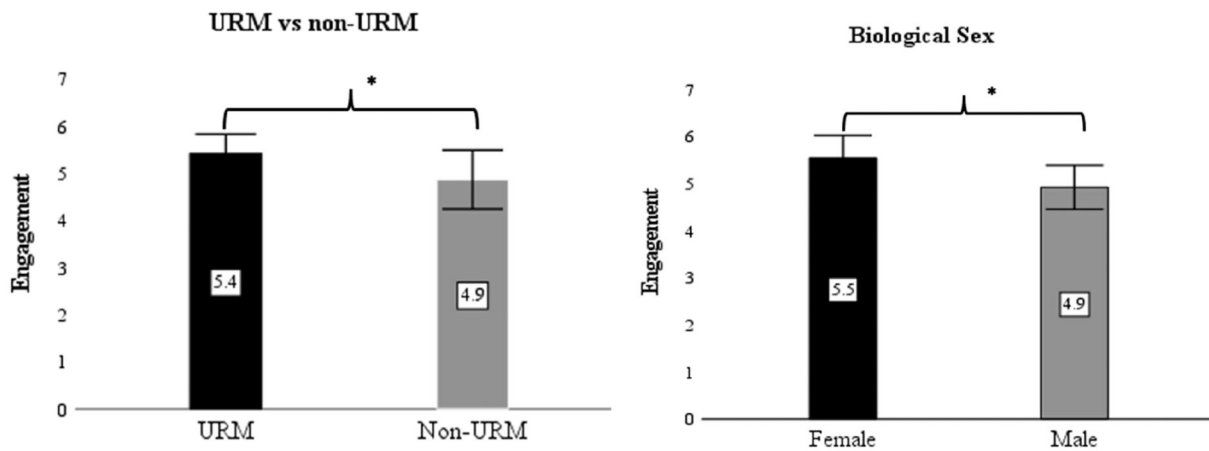
URM vs non-URM

Biological Sex

Figure 2. Engagement by groups.
Note. * Represents significant differences.
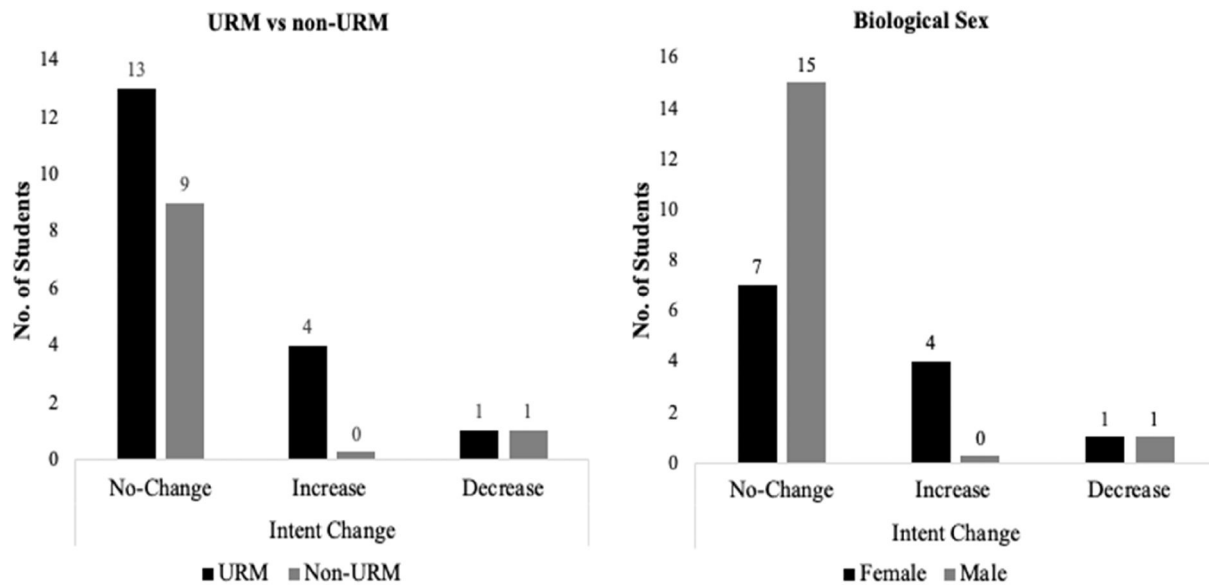
URM vs non-URM

Biological Sex

Figure 3. Trends of change in intent to pursue cybersecurity by group.

Table 2. Positive reactions and negative reactions.

Positive reaction			Negative reaction		
	n			*n*	
Theme	URM	non-URM	Theme	URM	non-URM
Coding and hacking	7	2	Technology failures	4	1
Learning	1	3	Lecture	2	–
Controlling the car	4	1	Losing the competition	1	1
Teamwork	2	–	Insufficient time	1	1
Competition	2	–			

4.4. Learner reactions to the activity

As the participants' reactions to the lesson/activity were qualitative, the data were analyzed using a thematic analysis approach (Braun & Clarke, 2006). The questions were categorized into positive and negative reactions, and the participants' responses were aligned with them. The data was then coded to identify similar responses. Codes were identified as they emerged and those that recurred were developed into themes. See Table 2 for positive and negative reactions, respectively, and the corresponding themes and frequencies. Due to the

limited sample size, the results were only compared between URM and non-URMs. Overall, more URMs cited more positive reactions about the lesson compared to non-URMs. On the other hand, more URMs quoted more negative reactions about the lesson compared to non-URMs. The majority of the negative reactions were tied to the defects in the technology, followed by the length of the lecture period when learners had the least interactivity with the RC car, computer, and software.

5. Discussion

The following sections summarize the findings and present a discussion of the theoretical and practical implications and future research considerations.

5.1. Summary of findings

The results of this study indicate that the participants experienced moderate levels of difficulty, perceived skills, and balance between difficulty and skills. Further, there were no

statistical differences in difficulty experienced during the task, perceived skills, or perceived balance between URM and non-URM nor males and females. The results also revealed high levels of engagement for all participants. In particular, females experienced significantly higher engagement levels than males, and URMs experienced significantly higher engagement than non-URMs. Finally, the results indicated a positive change in intent to pursue cybersecurity by female participants after participation in the lesson and the activity that was significantly greater than males.

5.2. Theoretical implications

5.2.1. Challenge-Skill match

Challenge-skill optimization in learning is important because research supports that it yields higher engagement, motivation, and positive learning outcomes when the challenge is optimized to the learners' skill set (Paas et al., 2005; Shernoff & Csikszentmihalyi, 2009). Carroll et al. (2021) opined that the challenge of the task is an aspect that can be modulated to enhance learner engagement. We aimed to create a module that would provide an appropriate challenge-skill match for URMs in high school by leveraging two key techniques. First, we couched the Network Traffic Analysis activity in a meaningful tool to students, specifically an IoT device in the form of an RC car. Prior research has found that female students and minorities commonly found Computer Science-related content to be too difficult likely due to the lack of prior exposure (Varma, 2010), however, the use of an IoT-based activity appeared to put all students on a relatively equal playing field and might have aided the perceived challenge-skill match because the IoT device provided a meaningful, relatable, and understandable learning experience. This is in line with extant research that has found that the utilization of IoT devices for cybersecurity instruction makes cybersecurity challenges and concepts more accessible to all learners compared to CTFs or other more expensive exercises (Chothia & De Ruiter, 2016). Second, the learning environment was loaded with researcher scaffolding throughout the activity, in the form of prompts and hints, as a way to provide guidance and encourage learners through any difficulties that they encountered. This likely helped learners to perceive difficulties as less challenging and more in line with their abilities. This is in congruence with extant research that has found that scaffolding yields an optimal challenge-skill match for learners (Kim et al., 2018). Further, learning research has shown the importance of instructor support as a critical factor for motivating minority students in cyber areas (Kornegay et al., 2021). Supportive teacher behavior was found to be a crucial dimension, influencing students' motivational beliefs, engagement, and achievement (Patrick et al., 2007; Yıldırım, 2012). Another aspect of the lesson that may have led to an optimal challenge-skill match was the collaborative nature of the learning environment. Extant research in learning has shown collaborative learning to foster perceived optimal challenge as it manifests peer scaffolding and irons out individual differences (Belland et al., 2013; Fan, 2015; Kim et al.,

2018). This is also supported by the theoretical framework of this study which proposed that interventions in the environment can positively influence learning outcomes (Carroll et al., 2021).

5.2.2. Learner engagement

The findings revealed that all participants experienced high levels of engagement during the module. These results are likely due in part to the use of an IoT device, the remote-controlled car, in the activity that created an experiential learning opportunity during which learners could see the practical impacts on the car when they applied the seemingly abstract concepts they had learned about in the lecture. This was also supported by the comments of the participants who rated controlling the car, and coding/hacking highly as positive experiences from the lesson. Extant research has found experiential learning to foster higher engagement and knowledge retention (Johnson et al., 2021; Stull & Mayer, 2007) and foster situational interest (Belland et al., 2013). Giannakas et al. (2022) also reported that a blended IoT device-based curriculum to teach students about encryption and decryption techniques was highly effective, efficient, satisfactory, and improved knowledge acquisition among participants. Further, the activity facilitated collaboration and hands-on experience for learners. This was supported by comments from participants when they reported having enjoyed the team experience. Collaborative learning experiences have been shown to enhance engagement in learning (Plauska & Damaševičius, 2014). The perceived challenge-skill match may have also contributed to higher levels of engagement experienced by the participants. Challenge-skill match has been found to increase learner engagement when the difficulty of the learning experience provides an adequate challenge for stimulation without leading to frustration or boredom (Barry Issenberg et al., 2005; Carroll et al., 2021; Nakamura & Csikszentmihalyi, 2002).

The findings also revealed significantly higher engagement levels for females than males and significantly higher engagement for URMs than non-URMs. These results might be attributed to several characteristics of the lesson such as embedding URM-focused instructional strategies. First, the collaborative characteristics of the tasks likely contributed to high levels of engagement in females and URMs as supported by the teamwork comments received as positive reactions about the lesson from URMs. Extant research in cybersecurity education has also shown that females prefer and are more engaged in creative collaborative training settings (Jethwani et al., 2017; Reychav & McHaney, 2017; Sax et al., 2017) and collaborative learning has been linked to increased motivation for African American learners in cybersecurity-related areas (Kornegay et al., 2021). Moreover, using collaborative tools for learning in Computer Science classrooms was found to create a friendly learning environment that was less intimidating to minority students (Avery et al., 2010). Second, the presence of minorities within the research team who provided support to the various teams may have also contributed to the high levels of engagement for URMs. Out of the nine researchers, six

were female of which two were Hispanic and one was Black. Research has found that having female instructors present in cybersecurity instruction can help younger female learners debunk the misconceptions and stereotypes about the domain of cybersecurity being male-dominated, and spark their interest (Ashcraft et al., 2012; Cheryan et al., 2013; Master et al., 2016), and the lack of role models was cited as a factor for low self-efficacy among females during Computer Science training (Zimmerman et al., 2011). Another explanation for significantly higher reports of engagement among females can be gleaned from their reactions to the activity. More female participants commented that the desire to learn about coding and hacking were aspects of cybersecurity that encouraged them to participate. This is in line with Jethwani et al. (2017) who opined that girls might be attracted to cybersecurity due to the practical application of hacking and coding skills.

5.2.3. Intent to pursue cybersecurity

The significant increase in female intent to pursue cybersecurity compared to males could be attributed to the collaborative learning strategy utilized to deliver the Network Traffic Analysis module. This is in line with extant research that has found that the use of a group challenge demonstrates the social aspects of cybersecurity and the requirement for collaborative performance, hence clearing misconceptions that the field is a solitary pursuit that lacks social benefit (Shumba et al., 2013). Extant research has also shown that when women do not find the social value of a profession, they tend to have a negative attitude toward it, but when a domain's social aspect is explicitly demonstrated, they are likely to gain interest (Cheryan et al., 2015; Harackiewicz et al., 2016; Hurtado et al., 2009; Johnson et al., 2021; Sax et al., 2017; Shumba et al., 2013; Weston et al., 2020). The attention hook that we utilized which was of a US military drone hacking scenario could have influenced the female students' intent to pursue cybersecurity. This is because, with such a scenario, the public relevance of protecting others through learning cybersecurity hacking skills was exemplified. Further, social learning environments were reported more favorable to females (Sax et al., 2017; Toda et al., 2019). Another contributor to these results might have been the presence of representative researchers (e.g., both females and minorities), during the study, which may have helped female and URM students to feel that the lesson and activity were attainable. This is in line with extant research that has reported that URMs find inspiration, motivation, and encouragement from other role models who look like them (Kricorian et al., 2020; Rowland, 2018). It is also probable that the female participants who reported an increase in intent to pursue cybersecurity after the lesson may have originally been disinterested due to indifference or lack of awareness of the discipline. This aligns with research that has found that females have more negative perspectives on Computer Science-related professions compared to males (McEwan & McConnell, 2013; McGill et al., 2016). However, once they experienced all the facets of the Network Traffic Analysis lesson, it could have

clarified some of their thoughts or doubts, built their self-efficacy through scaffolding techniques that were implemented, and changed their attitudes toward the discipline. Another social factor could have been the reassurance obtained through peer-to-peer interaction which is a noteworthy factor in students' initial pursuit of a course and the development of the associated self-efficacy (Hwang et al., 2015; Weston et al., 2020).

When examining the lack of significance in the change in intent to pursue cybersecurity found for URMs, it is probable that for other minorities such as African Americans and Hispanics, potentially the activity was not enough to make an impactful change in their intent to pursue cybersecurity. This could be attributed to the limitation of the study being concluded within a 45-minute class period. This constraint on time may have been insufficient for the module to have a meaningful impact on their intent to make long-term education or career decisions. A future longitudinal study could better address this research question.

5.3. Practical implications

There are several practical implications of the results of this evaluation of an IoT-based education approach to engage and educate URMs in cybersecurity, both for cybersecurity education and STEM, and are delineated below.

Leveraging meaningful technology that provides hands-on experience may ensure appropriate difficulty levels and increase learner engagement. When instructing and designing for younger learners in cybersecurity and Computer Science-related disciplines, instructors should ensure that the lecture portion of instruction that covers theoretical knowledge is sufficiently balanced with hands-on, experiential learning to allow students to see the practical implications of the abstract concepts they learn in lectures. Participants echoed controlling the car, coding, and hacking as some of the best experiences of the lesson. IoT devices provide a myriad of options for effective experiential learning and allow learners opportunities to interact with the hardware and software that they are familiar with. Integration of hands-on experience may lead to increased engagement levels during training.

Optimizing learners' challenge-skill match can ensure optimal difficulty levels, facilitate self-efficacy, and lead to more engagement and interest in a discipline. High school instructors should consider optimizing the material, assignments, and tasks to the learner's skills to promote engagement and arousal and prevent creating frustration or boredom when teaching younger learners about cybersecurity. Key to this is leveraging technology platforms, such as IoT devices that are familiar to most learners and for which learners have pre-existing knowledge schemas that can facilitate learning of new concepts. Further, instructors can utilize a scaffolding approach in which hints and prompts are provided adaptively to nudge learners toward the right solution to a challenge, reducing the frequency of these as the necessity wanes.

Utilizing collaborative learning activities can promote female engagement and interest in technical disciplines. Cybersecurity and STEM curricula should incorporate collaborative activities within instruction, for instance, group problem-solving and group competition. This can be easily achieved through the use of IoT devices, such as mobile devices. Further, groups should be limited to small numbers, for instance, four to five individuals to promote individual contribution within the group and an opportunity for individual learners within each group to interact with the instructional tools provided. Such collaborative learning experiences may help pique female and URM interest and engagement in STEM-related fields.

Redefining success may also help change the negative perception that females and minorities have regarding competitive learning environments in cybersecurity. During educational competitions, it may be beneficial to use alternative definitions of success instead of winning and losing to reduce the perceived pressure from the learning environment. Alternative forms of success include the most interactive group, best-observed team collaboration, and most innovative team. Participants echoed that losing the race was one of the things they disliked about the activity. Very competitive learning environments have been reported to discourage URMs from pursuing Computer Science-related courses, therefore creating opportunities to succeed that redefine performance into growth assessment can help students enjoy competitive learning environments.

The use of scaffolding techniques can help to optimize difficulty levels. Instructors are encouraged to teach new material and concepts in incremental levels, pushing the students beyond their current knowledge, while offering guidance and supportive feedback, and prompting learners towards autonomy. When learners have to apply the learned knowledge and skills in practice, instructors should be present to offer support and encourage more knowledgeable peers to assist struggling peers. Scaffolding can be further strengthened by utilizing IoT devices and other smart devices as instructional tools. Due to the fact that students may have already established familiarity with IoT devices, it can foster the transfer of knowledge and applicability of learned material.

6. Limitations and future research

The results of this study should be interpreted with caution given several limitations. The research was limited by the small sample size that consisted of only junior and senior high school students limiting applicability to other grades. Future research should examine the impact of IoT-based approaches on engagement and intent to pursue cybersecurity with a larger sample and broader age groups. Other sample characteristics to consider enhancing population validity include participants from diverse academic backgrounds, and college-level students, as results may differ for these demographics. Further, the lesson was of incredibly short duration, limiting the potential impacts. As already mentioned, the module was conducted in a 45-minute class period which might have limited the results to situational interest and hindered measuring URMs' interest in cybersecurity as a career path. Future research will attempt to evaluate the curriculum over an extended period to determine any changes and trends in participants' interest in a cybersecurity career and macro engagement in the material between lessons. Further, although the training may have sparked interest among female participants, it is difficult to determine whether the female students who found this renewed interest in cybersecurity would actually pursue a cybersecurity program at the college level or as a career. Future research should address these limitations by conducting a longitudinal study in which the same cohort of learners is studied throughout an entire training course over a long period to assess long-term effects. Given the limited duration, the lesson did not provide learners with the opportunity to see the several possibilities and applications of cybersecurity. Our future research is attempting to develop a cybersecurity curriculum with multiple modules that leverage a range of IoT devices and validated learning strategies designed to engage and educate URMs in cybersecurity. An evaluation of the entire curriculum spanning a semester will be conducted to assess learner outcomes. Furthermore, the study did not directly measure the influence of the presence of URMs or females as researchers on engagement, intent to pursue cybersecurity, and challenge-skill match, although it may have contributed to the female involvement during the study as a format of URM representation in cybersecurity instruction. Although this has been supported by literature, future research should attempt to capture and empirically measure how the presence of female instructors, role models, and mentors may impact the involvement of female students in the cybersecurity classroom.

7. Conclusion

In the current work, we aimed to design and evaluate the effectiveness of an IoT-based educational approach toward creating interest and increasing engagement in cybersecurity among URMs, including women, African Americans, and Hispanics. There has been a large diversity gap for these groups within the cybersecurity industry as it is currently dominated by Caucasian and Asian males. Many scholars have supported the need for diversity in the industry to tackle the novel type of cyber-attacks and tap into the benefits of diversity in the workplace. As such, we examined whether leveraging an IoT device, a hackable RC car, as a pedagogical tool, layered with instructional strategies that have proven effective at fostering URM engagement in Computer Science-related and STEM fields, was an effective method for cybersecurity instruction. Focusing on URMs in the cybersecurity industry, we further investigated whether this foundational cybersecurity module would increase high school learners' interest in and engagement in cybersecurity material. We examined if this approach achieved an optimal challenge/skill match for high school participants with limited knowledge of cybersecurity concepts, and if it led to

learner engagement and increased interest in cybersecurity among URMs. A lesson was implemented and evaluated using pre and post-measures. The results indicated a moderate challenge/skill balance for all groups, significantly higher levels of engagement among females compared to males and URMs versus non-URMs, and there was a significant difference in the number of females who reported an increase in their intent to pursue cybersecurity after exposure to the lesson, compared to males. The results are very promising and provide a foundation for further development of a high school-level cybersecurity curriculum using IoT devices to expose learners from underrepresented backgrounds to cybersecurity, foster their engagement during instruction, and potentially create and further their interest in the domain.

Acknowledgments

Disclosure statement

The authors report that there is no known conflict of interest that is financial or personal that could have influenced the work reported in this paper.

Funding

ORCID

Maureen Namukasa (iD) http://orcid.org/0000-0003-3158-2747

References

Abdel-Basset, M., Manogaran, G., Mohamed, M., & Rushdy, E. (2019). Internet of things in smart education environment: Supportive framework in the decision-making process. *Concurrency and Computation*, 31(10), e4515. https://doi.org/10.1002/cpe.4515

Air Force Association. (2022). Cyberpatriot XIV National Youth Cyber Defense Competition Registration Report 2021–2022. – Google Search. (n.d.). Retrieved 7 March 2023, from https://www.google.com/search?rlz=1C5CHFA_enQA870QA870&q=Air+Force+Association.+2022.+Cyberpatriot+XIV+National+Youth+Cyber+Defense+Competition+Registration+Report+2021-2022.&spell=1&sa=X&ved=2ahUKEwjw2Nya7cr9AhUpRDABHdQIB9UQBSgAegQICBAB&biw=830&bih=796&dpr=2

Arora, B. (2019). Teaching cyber security to non-tech students. *Politics*, 39(2), 252–265. https://doi.org/10.1177/0263395718760960

Ashcraft, C., Eger, E., Friend, M. (2012). Girls in IT: The facts. National Center for Women & IT. Boulder, CO. https://bcwt.bg/wp-content/uploads/documents/girlsInIT.pdf.

Avery, Z., Castillo, M., Guo, H., Guo, J., Warter-Perez, N., Won, D. S., Dong, J. (2010, October). Implementing collaborative project-based learning using the Tablet PC to enhance student learning in engineering and computer science courses. In *2010 IEEE Frontiers in Education Conference (FIE)* (pp. F1E-1.). IEEE. https://doi.org/10.1109/FIE.2010.5673215

Balakrishnan, B., & Low, F. S. (2016). Learning experience and socio-cultural influences on female engineering students' perspectives on engineering courses and careers. *Minerva*, 54(2), 219–239. https://doi.org/10.1007/s11024-016-9295-8

Ban, Y., Okamura, K., Kaneko, K. (2017). July). Effectiveness of experiential learning for keeping knowledge retention in IoT security education. In *2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)* (pp. 699–704.). Ieee https://doi.org/10.1109/IIAI-AAI.2017.206

Barry Issenberg, S., Mcgaghie, W. C., Petrusa, E. R., Lee Gordon, D., & Scalese, R. J. (2005). Features and uses of high-fidelity medical simulations that lead to effective learning: A BEME systematic review. *Medical Teacher*, 27(1), 10–28. https://doi.org/10.1080/01421590500046924

Belland, B. R., Kim, C., & Hannafin, M. J. (2013). A Framework for designing scaffolds that improve motivation and cognition. *Educational Psychologist*, 48(4), 243–270. https://doi.org/10.1080/00461520.2013.838920

Beveridge, R. (2021). Addressing the gender gap in the cybersecurity workforce. *International Journal of Cyber Research and Education*, 3(2), 54–61. https://doi.org/10.4018/IJCRE.2021070105

Bloom, B. S. (1976). *Human characteristics and school learning*. McGraw-Hill.

Bradberry, L. A., & De Maio, J. (2019). Learning by doing: The long-term impact of experiential learning programs on student success. *Journal of Political Science Education*, 15(1), 94–111. https://doi.org/10.1080/15512169.2018.1485571

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Burd, B., Barker, L., Divitini, M., Perez, F. A. F., Russell, I., Siever, B., Tudor, L. (2018, January). Courses, content, and tools for internet of things in computer science education. In *Proceedings of the 2017 ITiCSE Conference on Working Group Reports* (pp. 125–139.). https://doi.org/10.1145/3174781.3174788

Burrell, D. N. (2020). An exploration of the cybersecurity workforce shortage. In *Cyber warfare and terrorism: Concepts, methodologies, tools, and applications* (pp. 1072–1081). IGI Global. https://doi.org/10.4018/978-1-7998-2466-4.ch063

Carlson, S., Maxa, S. (1998). Pedagogy applied to nonformal education. http://conservancy.umn.edu/handle/11299/125490.

Carroll, M., Lindsey, S., Chaparro, M., & Winslow, B. (2021). An applied model of learner engagement and strategies for increasing learner engagement in the modern educational environment. *Interactive Learning Environments*, 29(5), 757–771. https://doi.org/10.1080/10494820.2019.1636083

Cherry, D., Cummings, R. T., Moon, D., Gosha, K. (2020). Exploring Computing Career Recruitment Strategies and Preferences for Black Computing Undergraduates at HBCUs. In *Proceedings of the 2020 ACM Southeast Conference* (pp. 47–54.). https://doi.org/10.1145/3374135.3385269

Cheryan, S., Drury, B. J., & Vichayapai, M. (2013). Enduring influence of stereotypical computer science role models on women's academic aspirations. *Psychology of Women Quarterly*, 37(1), 72–79. https://doi.org/10.1177/0361684312459328

Cheryan, S., Master, A., & Meltzoff, A. N. (2015). Cultural stereotypes as gatekeepers: Increasing girls' interest in computer science and engineering by diversifying stereotypes. *Frontiers in Psychology*, 6. https://doi.org/10.3389/fpsyg.2015.00049

Chiu, T. K. (2021). Digital support for student engagement in blended learning based on self-determination theory. *Computers in Human Behavior*, 124(2021), 106909. https://doi.org/10.1016/j.chb.2021.106909

Chothia, T., De Ruiter, J. (2016). Learning from {Others'} mistakes: Penetration testing {IoT} devices in the classroom. In *2016 USENIX Workshop on Advances in Security Education (ASE 16)*.

Chounta, I. A. (2020). Collaborative learning and patterns of practice. In *Encyclopedia of education and information technologies* (pp. 310–323). Springer International Publishing. https://doi.org/10.1007/978-3-030-10576-1_83

Cobb, S. (2018). "I'd like Y'all to get a black friend": The politics of race in friends. *Television & New Media*, 19(8), 708–723. https://doi.org/10.1177/1527476418778420

Csikszentmihalyi, M. (2014). Flow and education. In *Applications of Flow in Human Development and Education*. Springer. https://doi.org/10.1007/978-94-017-9094-9_6

Daud, F. (2022). *Benefits of teaching technology through experiential learning: Exploring the experiences of students of color* [Doctoral dissertation]. University of Kansas.

Delle Fave, A. (2013). Past, present, and future of flow. In I. Boniwell, S. A. David, & A. Conley A. (Eds.), *Oxford handbook of happiness* (2013; online edn). Oxford Academic. https://doi.org/10.1093/oxfordhb/9780199557257.013.0005.

Deterding, S., Sicart, M., Nacke, L., O'Hara, K., & Dixon, D. (2011). Gamification. Using game-design elements in non-gaming contexts. In *CHI'11 Extended Abstracts on Human Factors in Computing Systems* (pp. 2425–2428). https://doi.org/10.1145/1979742.1979575

Dillenbourg, P. (1999). *Collaborative learning: Cognitive and computational approaches. advances in learning and instruction series*. Elsevier Science, Inc. PO Box 945 10160-0757.

Dunn, M. H., Merkle, L. D. (2018, February). Assessing the impact of a national cybersecurity competition on students' career interests. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education* (pp. 62–67.). https://doi.org/10.1145/3159450.3159462

Eccles, J., Wigfield, A., Harold, R. D., & Blumenfeld, P. (1993). Age and gender differences in children's self-and task perceptions during elementary school. *Child Development*, 64(3), 830–847. https://doi.org/10.1111/j.1467-8624.1993.tb02946.x

Engeser, S., & Rheinberg, F. (2008). Flow, performance and moderators of challenge-skill balance. *Motivation and Emotion*, 32(3), 158–172. https://doi.org/10.1007/s11031-008-9102-4

Ericson, B. (2016). Detailed race and gender information 2015. http://home.cc.gatech.edu/ice-gt/594.

Esin, J. O. (2020). A call for concern: The unbalanced representation of minorities and women in cybersecurity profession. *J Women Minor Technol*, 2, 1–11.

Fan, Y.-C. (2015). Fostering learner autonomy through a socio-cognitive model of reading comprehension instruction. *British Journal of Education, Society & Behavioural Science*, 9(2), 105–117. https://doi.org/10.9734/BJESBS/2015/18161

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020). Teaching and learning iot cybersecurity and vulnerability assessment with shodan through practical use cases. *Sensors*, 20(11), 3048. https://doi.org/10.3390/s20113048

Giannakas, F., Troussas, C., Krouska, A., Voyiatzis, I., & Sgouropoulou, C. (2022). Blending cybersecurity education with IoT devices: A u-Learning scenario for introducing the man-in-the-middle attack. *Information Security Journal*, 32(5), 371–382. https://doi.org/10.1080/19393555.2022.2100297

Gray, T., & Ross, C. (2020). *The effects of an experiential learning course on secondary student achievement and motivation in Geometry* [Doctoral dissertation]. University of Missouri-Saint Louis.

Hamari, J., & Koivisto, J. (2014). Measuring flow in gamification: Dispositional flow scale-2. *Computers in Human Behavior*, 40(2014), 133–143. https://doi.org/10.1016/j.chb.2014.07.048

Hamari, J., Koivisto, J., Sarsa, H. (2014). Does gamification work? – A literature review of empirical studies on gamification. In 2014 47th Hawaii International Conference on System Sciences, 3025–3034. IEEE. https://doi.org/10.1109/HICSS.2014.377

Hamari, J., Shernoff, D. J., Rowe, E., Coller, B., Asbell-Clarke, J., & Edwards, T. (2016). Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning. *Computers in Human Behavior*, 54(2016), 170–179. https://doi.org/10.1016/j.chb.2015.07.045

Harackiewicz, J. M., Smith, J. L., & Priniski, S. J. (2016). Interest matters: The importance of promoting interest in education. *Policy Insights from the Behavioral and Brain Sciences*, 3(2), 220–227. https://doi.org/10.1177/2372732216655542

Hosaka, M. (2014). Women's experiences in the engineering laboratory in Japan. *European Journal of Engineering Education*, 39(4), 424–431. https://doi.org/10.1080/03043797.2014.883354

Hoyne, G., Alessandrini, J., & Fellman, M. (2016). Doctoral education for the future: Through the looking glass. In *Emerging directions in doctoral education* (Innovations in Higher Education Teaching and Learning, Vol. 6, pp. 21–38). Emerald Group Publishing Limited. https://doi.org/10.1108/S2055-364120160000006010

Huang, Y. M., & Chiu, P. S. (2015). The effectiveness of a meaningful learning-based evaluation model for context-aware mobile learning. *British Journal of Educational Technology*, 46(2), 437–447. https://doi.org/10.1111/bjet.12147

Hurtado, S., Cabrera, N. L., Lin, M. H., Arellano, L., & Espinosa, L. L. (2009). Diversifying science: Underrepresented student experiences in structured research programs. *Research in Higher Education*, 50(2), 189–214. https://doi.org/10.1007/s11162-008-9114-7

Hwang, G.-J., Lai, C.-L., & Wang, S.-Y. (2015). Seamless flipped learning: A mobile technology-enhanced flipped classroom with effective learning strategies. *Journal of Computers in Education*, 2(4), 449–473. https://doi.org/10.1007/s40692-015-0043-0

Iosup, A., & Epema, D. (2014). An experience report on using gamification in technical higher education. In Proceedings of *the 45th ACM Technical Symposium on Computer Science Education*. https://doi.org/10.1145/2538862.2538899

Jethwani, M. M., Memon, N., Seo, W., & 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

Jin, G., Tu, M., Kim, T.-H., Heffron, J., White, J. (2018). Game based cybersecurity training for high school students. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, 68–73. https://doi.org/10.1145/3159450.3159591

Jin, Y., Sun, J., Ma, H., Wang, X. (2021, December). The impact of different types of scaffolding in project-based learning on girls' computational thinking skills and self-efficacy. In *2021 Tenth International Conference of Educational Innovation through Technology (EITT)* (pp. 362–366). IEEE. https://doi.org/10.1109/EITT53287.2021.00077

Johnson, A. E., Barrack, J., Fitzgerald, J. M., Sobieraj, D. M., & Holle, L. M. (2021). Integration of a virtual dispensing simulator "MyDispense" in an experiential education program to prepare students for community introductory pharmacy practice experience. *Pharmacy*, 9(1), 48. https://doi.org/10.3390/pharmacy9010048

Kang, H., Calabrese Barton, A., Tan, E., D Simpkins, S., Rhee, H. Y., & Turner, C. (2019). How do middle school girls of color develop STEM identities? Middle school girls' participation in science activities and identification with STEM careers. *Science Education*, 103(2), 418–439. https://doi.org/10.1002/sce.21492

Kim, N. J., Belland, B. R., & Axelrod, D. (2018). Scaffolding for optimal challenge in K–12 problem-based learning. *Interdisciplinary Journal of Problem-Based Learning*, 13(1), 1712. https://doi.org/10.7771/1541-5015.1712

Konak, A. (2018). Experiential learning builds cybersecurity self-efficacy in K-12 students. *Education, Research and Practice, Journal of Cybersecurity*, 2018(1), 6. https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss1/6

Kornegay, M. A., Arafin, M. T., & Kornegay, K. (2021, July). Engaging underrepresented students in cybersecurity using Capture-the-Flag (CTF) competitions (experience). In *2021 ASEE Virtual Annual Conference Content Access*. https://peer.asee.org/37048

Kricorian, K., Seu, M., Lopez, D., Ureta, E., & Equils, O. (2020). Factors influencing participation of underrepresented students in STEM fields: Matched mentors and mindsets. *International Journal of STEM Education*, 7(1), 1–9. https://doi.org/10.1186/s40594-020-00219-2

Laal, M., & Laal, M. (2012). Collaborative learning: What is it? *Procedia – Social and Behavioral Sciences*, 31(2012), 491–495. https://doi.org/10.1016/j.sbspro.2011.12.092

Laskowski, M., & Badurowicz, M. (2014). Gamification in higher education: A case study. Human capital without borders: Knowledge

and learning for quality of life. In *Proceedings of the management, knowledge and learning international conference*.

Leune, K., & Petrilli, S. J. (2017). Using Capture-the-Flag to enhance the effectiveness of cybersecurity education. In Proceedings of the. In *18th Annual Conference on Information Technology Education*, 47–52. https://doi.org/10.1145/3125659.3125686

Li, L. (2022). Reskilling and upskilling the future-ready workforce for industry 4.0 and Beyond. *Information Systems Frontiers*, 1–16. https://doi.org/10.1007/s10796-022-10308-y

Lietaert, S., Roorda, D., Laevers, F., Verschueren, K., & De Fraine, B. (2015). The gender gap in student engagement: The role of teachers' autonomy support, structure, and involvement. *The British Journal of Educational Psychology*, 85(4), 498–518. https://doi.org/10.1111/bjep.12095

Lingelbach, K. K. (2018). *Perceptions of female cybersecurity professionals toward factors that encourage females to the cybersecurity field* [Doctoral dissertation]. Nova Southeastern University.

Mäenpää, H., Tarkoma, S., Varjonen, S., Vihavainen, A. (2015, February). Blending problem-and project-based learning in internet of things education: Case greenhouse maintenance. In *Proceedings of the 46th ACM Technical Symposium on Computer Science Education* (pp. 398–403). https://doi.org/10.1145/2676723.2677262

Malecki, A. (2018). Cybersecurity in the classroom: Bridging the gap between computer access and online safety. https://scholar.valpo.edu/cscrpr/1.

Master, A., Cheryan, S., & Meltzoff, A. N. (2016). Computing whether she belongs: Stereotypes undermine girls' interest and sense of belonging in computer science. *Journal of Educational Psychology*, 108(3), 424–437. https://doi.org/10.1037/edu0000061

McEwan, T., McConnell, A. (2013, October). Young people's perceptions of computing careers. In *2013 IEEE Frontiers in Education Conference (FIE)* (pp. 1597–1603). IEEE. https://doi.org/10.1109/FIE.2013.6685108

McGill, M. M., Decker, A., & Settle, A. (2016). Undergraduate students' perceptions of the impact of pre-college computing activities on choices of major. *ACM Transactions on Computing Education*, 16(4), 1–33. https://doi.org/10.1145/2920214

Mirkovic, J., Peterson, P. (2014). Class Capture-the-Flag exercises. 3GSE. Retrieved from https://www.usenix.org/conference/3gse14/summit-program/presentation/mirkovic.

Mountrouidou, X., Vosen, D., Kari, C., Azhar, M. Q., Bhatia, S., Gagne, G., Maguire, J., Tudor, L., Yuen, T. T. (2019). Securing the human: A review of literature on broadening diversity in cybersecurity education. *Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education*, 157–176. https://doi.org/10.1145/3344429.3372507

Mubarok, H., Sofia, N., Kristina, D., & Rochsantiningsih, D. (2022). Meaningful Learning Model: The impact on students' reading comprehension. *Journal of Educational and Social Research*, 12(1), 346–354. https://doi.org/10.36941/jesr-2022-0027

Nakamura, J., & Csikszentmihalyi, M. (2002). The concept of flow. *Handbook of Positive Psychology*, 89, 105.

Nygard, K., Chowdhury, M., Kambhampaty, K., Kotala, P. (2018, April). Cybersecurity materials for K-12 education. The Midwest Instruction and Computing Symposium 2018. Retrieved from https://micsymposium.org/mics2018/proceedings/MICS_2018_paper_59.pdf.

Ošlejšek, R., Rusňák, V., Burská, K., Švábenský, V., & Vykopal, J. (2019). Visual feedback for players of multi-level Capture the Flag games: Field usability study. In *2019 IEEE Symposium on Visualization for Cyber Security (VizSec)*, 1–11. https://doi.org/10.1109/VizSec48167.2019.9161386

Osman, M. C., Namukasa, M., Ficke, C., Piasecki, I., OConnor, T. J., & Carroll, M. (2023). Understanding how to diversify the cybersecurity workforce: A qualitative analysis. *Journal of Cybersecurity Education, Research, and Practice*, 2023(2), 4. https://digitalcommons.kennesaw.edu/jcerp/vol2023/iss2/4/

Paas, F., Tuovinen, J. E., van Merriënboer, J. J. G., & Aubteen Darabi, A. (2005). A motivational perspective on the relation between mental effort and performance: Optimizing learner involvement in instruction. *Educational Technology Research and Development*, 53(3), 25–34. https://doi.org/10.1007/BF02504795

Patrick, H., Ryan, A. M., & Kaplan, A. (2007). Early adolescents' perceptions of the classroom social environment, motivational beliefs, and engagement. *Journal of Educational Psychology*, 99(1), 83–98. https://doi.org/10.1037/0022-0663.99.1.83

Peacock, D., & Irons, A. (2017). Gender inequality in cybersecurity: Exploring the gender gap in opportunities and progression. *International Journal of Gender, Science and Technology*, 9(1), 25–44. https://genderandset.open.ac.uk/index.php/genderandset/article/view/449

Pedro, L. Z., Lopes, A. M., Prates, B. G., Vassileva, J., Isotani, S. (2015). Does gamification work for boys and girls? An exploratory study with a virtual learning environment. In *Proceedings of the 30th Annual ACM Symposium on Applied Computing*, 214–219. https://doi.org/10.1145/2695664.2695752

Petersen, R., Santos, D., Smith, M., & Witte, G. (2020). *Workforce framework for cybersecurity (NICE framework)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181r1

Pietri, E. S., Johnson, I. R., Majid, S., & Chu, C. (2021). Seeing what's possible: Videos are more effective than written portrayals for enhancing the relatability of scientists and promoting black female students' interest in STEM. *Sex Roles*, 84(1–2), 14–33. https://doi.org/10.1007/s11199-020-01153-x

Pinchot, J., Cellante, D., Mishra, S., & Paullet, K. (2020). Student Perceptions of Challenges and Role of Mentorship in Cybersecurity Careers: Addressing the Gender Gap. *Information Systems Education Journal*, 18(3), 44–53. https://eric.ed.gov/?id=EJ1258205

Plauska, I., & Damaševičius, R. (2014, October 9–10, 2014). Educational robots for internet-of-things supported collaborative learning. In *Information and Software Technologies: 20th International Conference, ICIST 2014*, Druskininkai, Lithuania. Proceedings 20 (pp. 346–358). Springer International Publishing. https://doi.org/10.1007/978-3-319-11958-8_28

Pöysä, S., Vasalampi, K., Muotka, J., Lerkkanen, M. K., Poikkeus, A. M., & Nurmi, J. E. (2019). Teacher–student interaction and lower secondary school students' situational engagement. *The British Journal of Educational Psychology*, 89(2), 374–392. https://doi.org/10.1111/bjep.12244

Preston, E. (2023). *Lack of black female diversity within the cybersecurity workforce*. Old Dominion University Digital Commons. https://doi.org/10.25776/k9m2-2r57

Procci, K., Singer, A. R., Levy, K. R., & Bowers, C. (2012). Measuring the flow experience of gamers: An evaluation of the DFS-2. *Computers in Human Behavior*, 28(6), 2306–2312. https://doi.org/10.1016/j.chb.2012.06.039

Renninger, K. A., & Hidi, S. E. (2015). *The power of interest for motivation and engagement*. Routledge. https://doi.org/10.4324/9781315771045

Reychav, I., & McHaney, R. (2017). The relationship between gender and mobile technology use in collaborative learning settings: An empirical investigation. *Computers & Education*, 113, 61–74. https://doi.org/10.1016/j.compedu.2017.05.005

Rheinberg, F., Vollmeyer, R., & Engeser, S. (2003). Die erfassung des flow-erlebens [The assessment of flow experience]. In J. Stiensmeier-Pelster & F. Rheinberg (Eds.), *Diagnostik von Motivation und Selbstkonzept* (pp. 261–279). Hogrefe.

Riley, M., Elgin, B., Lawrence, D., Matlack, C. (2014, March 17). Missed alarms and 40 million stolen credit card numbers: How Target blew it. Bloomberg.Com. https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data.

Rockinson-Szapkiw, A., Wendt, J. L., & Stephen, J. S. (2021). The efficacy of a blended peer mentoring experience for racial and ethnic minority women in STEM pilot study: Academic, professional, and psychosocial outcomes for mentors and mentees. *Journal for STEM Education Research*, 4, 1–21. https://doi.org/10.1007/s41979-020-00048-6

Rowland, P. (2018). The CybHER program supported by CISSE framework to engage and anchor middle-school girls in cybersecurity. https://scholar.dsu.edu/theses/337.

Sax, L. J., Lehman, K. J., Jacobs, J. A., Kanny, M. A., Lim, G., Monje-Paulson, L., & Zimmerman, H. B. (2017). Anatomy of an enduring gender gap: The evolution of women's participation in computer science. *The Journal of Higher Education*, 88(2), 258–293. https://doi.org/10.1080/00221546.2016.1257306

Schmidt, H. G., Rotgans, J. I., & Yew, E. H. (2011). The process of problem-based learning: What works and why. *Medical Education*, 45(8), 792–806. https://doi.org/10.1111/j.1365-2923.2011.04035.x

Schneider, B., Krajcik, J., Lavonen, J., Salmela-Aro, K., Broda, M., Spicer, J., Bruner, J., Moeller, J., Linnansaari, J., Juuti, K., & Viljaranta, J. (2016). Investigating optimal learning moments in US and Finnish science classes. *Journal of Research in Science Teaching*, 53(3), 400–421. https://doi.org/10.1002/tea.21306

Shernoff, D. J., Csikszentmihalyi, M., Shneider, B., & Shernoff, E. S. (2003). Student engagement in high school classrooms from the perspective of flow theory. *School Psychology Quarterly*, 18(2), 158–176. https://doi.org/10.1521/scpq.18.2.158.21860

Shernoff, D. J. (2013). Optimal learning environments to promote student engagement. Springer.

Shernoff, D. J., & Anderson, B. (2014). *Enacting flow and student engagement in the college classroom* (pp. 194–212). The Wiley Blackwell Handbook of Positive Psychological Interventions.

Shernoff, D. J., & Csikszentmihalyi, M. (2009). Cultivating engaged learners and optimal learning environments. *Handbook of Positive Psychology in Schools*, 131, 145.

Shumba, R., Ferguson-Boucher, K., Sweedyk, E., Taylor, C., Franklin, G., Turner, C., Sande, C., Acholonu, G., Bace, R., & Hall, L. (2013, June). Cybersecurity, women and minorities: Findings and recommendations from a preliminary investigation. In *Proceedings of the ITiCSE working group reports conference on innovation and technology in computer science education-working group reports* (pp. 1–14). https://doi.org/10.1145/2543882.2543883

Simons, K. D., & Klein, J. D. (2007). The impact of scaffolding and student achievement levels in a problem-based learning environment. *Instructional Science*, 35(1), 41–72. https://doi.org/10.1007/s11251-006-9002-5

Strandberg-Long, P. (2021). Staying on task – How the concept of skill-challenge balance provides a key element to the teaching of the Meisner technique. *Stanislavski Studies*, 9(2), 163–184. https://doi.org/10.1080/20567790.2021.1969762

Stull, A. T., & Mayer, R. E. (2007). Learning by doing versus learning by viewing: Three experimental comparisons of learner-generated versus author-provided graphic organizers. *Journal of Educational Psychology*, 99(4), 808–820. https://doi.org/10.1037/0022-0663.99.4.808

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the Internet of Things: A Comprehensive Review. *Sensors*, 23(8), 4117. https://doi.org/10.3390/s23084117

Tse, D. C., Nakamura, J., & Csikszentmihalyi, M. (2020). Beyond challenge-seeking and skill-building: Toward the lifespan developmental perspective on flow theory. *The Journal of Positive Psychology*, 15(2), 171–182. https://doi.org/10.1080/17439760.2019.1579362

Tobey, D. H., Pusey, P., & Burley, D. L. (2014). Engaging learners in cybersecurity careers: Lessons from the launch of the national cyber league. *ACM Inroads*, 5(1), 53–56. https://doi.org/10.1145/2568195.2568213

Toda, A. M., Oliveira, W., Shi, L., Bittencourt, I. I., Isotani, S., Cristea, A. (2019). Planning gamification strategies based on user characteristics and DM: A dender-based case study (arXiv:1905.09146). arXiv. https://arxiv.org/abs/1905.09146.

Varma, R. (2010). Why so few women enroll in computing? Gender and ethnic differences in students' perception. *Computer Science Education*, 20(4), 301–316. https://doi.org/10.1080/08993408.2010.527697

Verenikina, I. (2003). Understanding scaffolding and the ZPD in educational research. Retrieved from https://ro.uow.edu.au/edupapers/381/.

Wahsheh, L. A., Mekonnen, B. (2019, December). Practical cyber security training exercises. In 2019 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 48–53). IEEE. https://doi.org/10.1109/CSCI49370.2019.00015

Walker, A., Leary, H., & Hmelo-Silver, C. (Eds.) (2015). *Essential readings in problem-based learning: Exploring and extending the legacy of Howard S. Barrows*. Purdue University Press.

Wang, L., & Chen, M. (2010). The effects of game strategy and preference-matching on flow experience and programming performance in game-based learning. *Innovations in Education and Teaching International*, 47(1), 39–52. https://doi.org/10.1080/14703290903525838

Werbach, K., & Hunter, D. (2015). *The gamification toolkit: Dynamics, mechanics, and components for the win*. University of Pennsylvania Press.

Weston, T. J., Dubow, W. M., & Kaminsky, A. (2020). Predicting women's persistence in Computer Science- and technology-related majors from high school to college. *ACM Transactions on Computing Education*, 20(1), 1–16. https://doi.org/10.1145/3343195

White, V., Alexander, J., Prince, D., & Verdell, A. (2018). The impact of student engagement, institutional environment, college preparation, and financial support on the persistence of underrepresented minority students in engineering at a predominately White institution: A perspective from students. *Journal of Higher Education Theory and Practice*, 18(2), 64. https://par.nsf.gov/biblio/10078664

Whitson, C., & Consoli, J. (2009). Flow theory and student engagement. *Journal of Cross-Disciplinary Perspectives in Education*, 2(1), 40–49.

Wigfield, A., & Eccles, J. S. (2000). Expectancy–value theory of achievement motivation. *Contemporary Educational Psychology*, 25(1), 68–81. https://doi.org/10.1006/ceps.1999.1015

Yıldırım, S. (2012). Teacher support, motivation, learning strategy use, and achievement: A multilevel mediation model. *The Journal of Experimental Education*, 80(2), 150–172. https://doi.org/10.1080/00220973.2011.596855

Zahedi, L., Batten, J., Ross, M., Potvin, G., Damas, S., Clarke, P., & Davis, D. (2021). Gamification in education: A mixed-methods study of gender on computer science students' academic performance and identity development. *Journal of Computing in Higher Education*, 33(2), 441–474. https://doi.org/10.1007/s12528-021-09271-5

Zimmerman, T. G., Johnson, D., Wambsgans, C., & Fuentes, A. (2011). Why Latino high school students select computer science as a major: Analysis of a success story. *ACM Transactions on Computing Education*, 11(2), 1–17. https://doi.org/10.1145/1993069.1993074

About the Authors

Maureen Namukasa is a PhD student of Aviation Sciences at Florida Tech and a research scientist at ATLAS Lab. She has a B.S. in Industrial Psychology and an M.S. in Aviation Human Factors. Her research areas include training development, human performance, human-centered design, and Advanced Air Mobility.

Maria Chaparro Osman received a BS in Technical Communication and New Media from the University of South Florida, an M.S. in Aviation Human Factors, and a PhD in Aviation Sciences from Florida Tech. Her research areas include decision-making in novel conditions, training, Advanced Air Mobility, and remote-controlled unmanned systems.

Cherrise Ficke received a BS in Aviation Management and an MS in Human Factors in Aeronautics from Florida Tech. She also holds a Private Pilot's License (PPL). Her research areas include decision-making, unmanned aerial systems (UAS) operations, human-agent teaming (HAT), augmented reality (AR), and virtual environments (VE).

Isabella Piasecki received a BS in Aviation Human Factors from Florida Tech's College of Aeronautics. She holds a Private Pilot's License (PPL) and her research background includes human-agent teaming (HAT) and training development.

TJ OConnor's research has centered on computer security, emphasizing cybersecurity education, the security and privacy of IoT devices, wireless protocols, and software-defined networking. He is active in cybersecurity competitions and is the current coach for the FITSec Cybersecurity Team and previously coached the US Cyber Games Team.

Meredith Carroll is a Professor of Aviation Human Factors at Florida Institute of Technology's College of Aeronautics. She has nearly 20 years of experience, both in industry and academia, studying human performance, human-computer interaction, and learning in complex systems within commercial aviation, military, and space applications.