To Hack or Not to Hack? Connecting Cybersecurity, the IoT, and Smart Environments to K12 Learning Experiences

Shusmoy Chowdhury[1], Debaleen Das Spandan[1], Tara Bonebrake[2], Zachary Frantsen[3], and Ajay Katangur[1]

[1] Department of Computer Science, Missouri State University, 901 S National Ave, Springfield, 65897, Missouri, USA
{shusmoy26, debaleen0010, ajaykatangur}@missouristate.edu
[2] The Summit Preparatory School, Springfield, USA
Tbonebrake@thesummitprep.org
[3] Marion C. Early High School, Springfield, USA
frantsen@mcestaff.com

Abstract. The Internet of Things (IoT) refers to the interconnectedness of devices within a network, while smart environments denote the interface between users and IoT through network capabilities. The widespread adoption of connected smart devices is projected to continue growing exponentially, benefiting businesses, households, and educational institutions. However, this growth also brings increased risks of security threats and privacy breaches associated with IoT. Users of smart environments may overlook, lack awareness of, or have insufficient resources to address these potential security risks effectively. Security challenges in the IoT encompass various threats such as data leakage, hacking, software vulnerabilities, device security, IoT exploitation, and denial of service attacks. Currently, security protocols in smart environments and IoT are fragmented, posing challenges for consistent protection against these threats. As security risks persist, there is a growing need for innovative cybersecurity education, especially in K-12 settings. This study conducted training sessions for high school teachers to educate them about IoT device security vulnerabilities through an NSF-RET grant. The aim was to impart this knowledge to students through their teachers. The curriculum and project designs resulting from the training generated significant interest among students. Moreover, feedback from student surveys indicated enhanced knowledge and increased practical understanding of IoT security concepts.

Keywords: Hack · IoT · K-12 · Security · Smart Devices

1 Introduction

The rapid advancement of information technology in recent decades has underscored the increasing significance of computational skills, particularly for the Science, Technology, Engineering, and Mathematics (STEM) workforce [21]. Currently, the United States ranks 17th in science and 25th in math among other

nations [31]. In engineering, China and India graduate many more engineers than the US [17]. In 2011, China's engineering graduates totaled 1,000,000 [10], compared to the US' 84,599 graduates [13].

K12 schools today live on the front lines of technological integration in all aspects of the community [37]. From the use of technology to support classroom instruction and information, to connect with the school community, to automating energy efficiency, schools are an platform for technology integration [35]. However, the typical K-12 curriculum often lacks substantial exposure to computational thinking, scientific computing, and research methodologies, particularly for students in grades 6-12 [8]. This deficiency hampers their ability to explore, design, and implement solutions for STEM projects within the classroom. Consequently, there arises a necessity to integrate additional STEM-oriented material within the K-12 curriculum with the aim of augmenting students' knowledge.

The concept of Internet of Things (IoT) encompasses the interconnectedness of devices, enabling communication and data exchange [30].The proliferation of connected devices globally, as projected by Statistica [36], is set to reach approximately 75.44 billion by 2025, marking a substantial increase from 30.73 billion in 2020 [2]. While this connectivity offers numerous advantages, including cost savings and improved operational efficiency, it also introduces vulnerabilities that must be addressed. This surge in Internet of Things (IoT) devices presents a vast playground for cybercriminals to exploit vulnerabilities [27]. Such vulnerabilities can lead to severe consequences, including unauthorized control of machinery, access to sensitive data like live audio/video feeds, and potential theft of crucial information if robust security measures are not in place.

Identifying and mitigating security vulnerabilities in the IoT domain poses a significant challenge, encompassing issues such as authentication gaps, lack of encryption, buffer overflow, and SQL injection [38]. Addressing these vulnerabilities is crucial for maintaining the confidentiality, integrity, and availability of data. Schools, as hubs of technological integration [12], must navigate these complexities to harness the full potential of IoT while mitigating security threats.

Schools are smart environment hubs providing a means to streamline school facilities usually with significant cost savings. One of the most common ways that computer science (CS)learning is incorporated into classroom practice through robots. In addition to this, using sensors to collect data and conduct research is supporting expansion of deeper learning in STEM. The use of technology to support school and district connections to families offers expanded communication opportunities. Positive impacts abound with the adoption of current technological trends creating a space for increased IoT connection.

In-depth comprehension of the IoT within the K-12 educational setting is paramount for maximizing advantages and devising effective strategies for securing IoT assets. Our focus has been on training high school teachers from Southwest Missouri to understand the vulnerabilities associated with IoT devices in the realm of security. Our research entailed a six-week training program conducted during the summer-2023 months. This training covered foundational networking concepts and progressed to addressing critical vulnerabilities inher-

ent in smart devices. Various attack scenarios, such as Denial of Service (DoS) and distributed denial-of-service (DDoS) attacks, were demonstrated. Additionally, anomalous behaviors exhibited by smart devices, which could compromise the safety and security of the IoT environment, were highlighted.

The training sessions as well as the research conducted by the teachers on IoT security elicited significant enthusiasm and interest among them. During the summer National Science Foundation (NSF) Research Experience for Teachers (RET) program named Research on Smart Environments (ROSE), they proceeded to develop curricula or lesson plans for the upcoming academic semester, incorporating insights gained from the training and research experience to be shared with their students in the classroom. Furthermore, the educators devised projects aimed at providing students in their classes with practical experience regarding security vulnerabilities in IoT devices and fostering the creation of strategies to mitigate these vulnerabilities. Ongoing monitoring of teachers implementation of the acquired knowledge in their classrooms is being conducted, ensuring the sustained integration of training into educational practices.

The subsequent sections of this paper are structured as follows: Section 2 provides an overview of prior research concerning the integration of computer science technologies in STEM and K-12 education. Section 3 presents a detailed explanation and overview of the methodology employed in our IoT security vulnerability training and research. Section 4 evaluates both the anticipated outcomes and the current status of our research implementation, as well as analyzes student interactions with our content. Finally, Section 5 offers a summary of our research, discusses our findings, and outlines potential avenues for future improvement in this area of research training.

2 Related Works

Various evidence-based CS curriculum such as CS10k are designed over the decade to engage students from different backgrounds in CS classroom [4]. Although these initiatives has great impact on the US education, there is a necessity of well prepared CS teachers. The well prepared teachers can effectively teach CS contents and address equity issue properly in CS classrooms [18]. Researchers consistently emphasize the significance of equipping educators with comprehensive CS content knowledge and promoting equitable pedagogical practices [18].

Satasha L. Green et al. [19] emphasize the significance of training K-12 educators in STEM fields using a multidisciplinary approach. They conducted a survey of over 150 students enrolled in the Advanced Certificate in STEM program using a questionnaire. The research gathered data on students' perceptions of enhanced knowledge and skills in STEM subjects following completion of the certificate program. The findings indicate improvement in the initial adoption of STEM concepts and the application of tools learned during the program.

Additionally, another study [16] proposed a video-game based learning strategy targeting children aged 8 to 12 years to enhance their awareness regarding strong password setup and identification of password-related vulnerabilities.

This approach integrated learning and entertainment, leveraging an application to increase students' interest and engagement in cybersecurity. Similarly, [20] introduced and evaluated a comparable game for cybersecurity, and digital literacy education among younger adults in Canada within a classroom setting. Furthermore, various research endeavors [24,32,1,28] have developed and advocated for different approaches, modules, and tools aimed at enhancing students' cybersecurity awareness. However, despite the existence of numerous programs and modules for educating children on cybersecurity awareness, there remains a gap in programs that utilize tools to develop awareness and professional skills among younger adults.

The turn of the 20th to the 21st century marked a significant shift in higher education, with institutions widely adopting technologies such as the Internet of Things (IoT), bring your own device (BYOD), wearable devices, and mobile learning devices (MLDs) as integral components of educational strategies [14,29,33]. These technologies, including learning management systems (LMS) commonly used in distance education, were embraced by academic institutions, scholars, and governments for enhancing pedagogical approaches, particularly in eLearning contexts [3,26,35]. However, the proliferation of cyber threats in online environments has underscored the need for comprehensive training and awareness regarding Acceptable Use Policies (AUP) among new hires, students, and staff members utilizing institutional networks [33]. The educational community must recognize the risks posed by cyber threats, including data theft, malicious attacks, and malware dissemination, and prioritize AUP awareness to mitigate these dangers [7,5,23,25].

Furthermore, the integration of IoT and wearable devices among online college and university students has heightened vulnerabilities in educational networks, making them susceptible to cyber threats. These devices, forming part of Information and Communication Technology (ICT) in education, utilize various interconnection protocols such as Wi-Fi, Bluetooth, or Ethernet via sensors, thereby increasing the complexity of network security [6,7,5,9].

The advent of Internet Protocol version 6 (IPv6) has further accelerated the adoption of IoT and wearable technology in education and healthcare sectors, but it has also raised concerns about the safety and security of MLDs, BYODs, and IoT devices when accessing application and data resources [11,34]. These devices are susceptible to hacking due to lapses in AUP adherence and other vulnerabilities, with human error being identified as a primary weak point in cybersecurity defenses within educational networks [15,34]. A lack of awareness regarding AUP guidelines and device functionalities among users contributes significantly to cybersecurity risks, emphasizing the urgent need for education and training in this domain [11,22].

3 Methodology

Our research focus is on smart environments, where sensors and actuators collect information about the physical world around us and tend to positively impact

our lives by offering automation, remote control, and interconnectedness. Our research purpose is to use smart IoT devices to analyze security vulnerabilities and attacks on them. The teachers were actively engaged in these NSF-RET projects and developed class-appropriate activities and materials for academic year implementation in their classroom.

3.1 Participants

Our research project is designed to serve middle (6-8) and high school (9-12) STEM teachers in Southwest Missouri, including rural school districts within an hour's distance from the MSU campus. We focused on recruiting teachers serving in schools with low-income and underrepresented groups of students. Our informational campaigns and selection rubric were geared towards attracting teachers with disabilities, veterans, African Americans, Hispanics, Latinos, and Native Americans. We received supporting letters from local districts/schools, such as Springfield (Kickapoo High School, Parkview High School) and Greenwood Laboratory School, as well as, rural schools, Dadeville (Dadeville High School), Marion County (Marion C. Early High School), Marshfield (Marshfield high school), and Pierce City (Pierce City High School).

3.2 Approach

The research methodology is shown in "Fig 1". We have divided our security contents for IoT devices into three differemnt categories.

To Hack or Not to Hack Initially, we delved into the foundational aspects of computer networks, instructing educators on diverse network typologies and elucidating terminologies including Domain Name Server (DNS), Address Resolution Protocol (ARP), Ethernet, and Local Area Network (LAN), among others. We introduced several network protocols, encompassing TCP/IP, UDP, ICMP, and elucidated the disparities between IPv4 and IPv6. In terms of network architecture, an exhaustive comparison between LAN and WAN was provided, discussing their respective utilities in varied settings such as domestic networks, educational institution networks, and the internet. A comprehensive analysis of the OSI model was conducted, delineating its seven layers and underscoring its significance in standardizing network communications.

Subsequently, we delved into an exploration of assorted tools for network analysis, including ping, tracert, Nmap, Wireshark, and Fing. This knowledge forms the bedrock of understanding within the security domain, equipping educators with a robust comprehension of security vulnerabilities. Hence, this segment of learning has been classified as essential for both defensive and offensive security training, encompassing both defensive strategies ("Not to Hack") and offensive tactics ("To Hack").

Not to Hack Upon establishing a foundational understanding of computer networks, our instructional focus transitioned towards elucidating the essential information pertinent to network penetration. The initial step in this process involves gaining access to the local network (Wi-Fi), which is imperative for the subsequent actions of hacking IoT devices or inducing anomalous behavior in connected devices. Upon successful entry into the local network, our attention turned to comprehensively understanding the network's topology. This phase necessitated a thorough network scan utilizing tools such as Nmap or Fing, enabling the acquisition of IP addresses associated with smart devices connected to the local network. Specifically, our research centered on tracking the IPv4 addresses of these smart devices. Moving forward, our strategy involved utilizing these obtained IP addresses to initiate hacking endeavors targeting the identified smart devices. This process encompasses not only accessing the devices but also manipulating them to exhibit desired behaviors, constituting a critical component of our investigative approach.

To Hack During the third week of the program, the curriculum shifted its focus towards Internet of Things (IoT) devices, with an emphasis on analyzing vulnerabilities across various devices. The instructional content emphasized the fundamental components requisite for "hacking." Participants were encouraged to undertake self-directed research, leveraging resources such as Exploit-DB and diverse search engines to identify vulnerable IoT devices such as smart lights, smart plugs, and door sensors. This exploration culminated in the introduction of the Kasa Smart bulb and Kasa Smart plug. Subsequently, participants engaged in understanding how to manipulate these smart devices using Python programming. Leveraging familiar tools like tracert, Nmap, Fing, and Wireshark, they conducted network scans to identify connected devices and collect pertinent data. Their task was to utilize this information to identify vulnerabilities or potential exploitation methods concerning these devices.

Following this, participants were introduced to a Python library designed for Kasa devices, prompting them to commence coding to potentially control these devices. Faculty members and graduate mentors guided in refining their code, leading to the successful manipulation of the Kasa plug and bulb. Participants were then encouraged to explore additional types of attacks that could be executed on these devices, further enhancing their autonomous research capabilities. Notably, participants independently acquired knowledge regarding Bluetooth device manipulation and the Man-in-the-Middle attack.

Furthermore, participants were tasked with conducting a literature review on smart locks, resulting in the discovery of a research paper detailing a smart lock hack involving reverse engineering, encryption, and Bluetooth packet capturing. Additionally, they were introduced to socket programming in Python and briefed on a Denial of Service (DoS) attack. A practical demonstration of a DoS attack was performed on one of the smart home plugs. Discussions also encompassed various other potential attacks capable of causing disruptions within smart home devices.

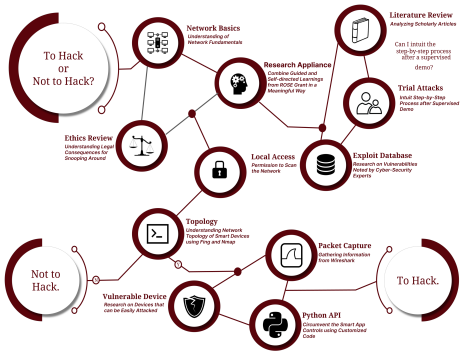


Fig. 1: Research Methodology for cyber-security training in IoT domain

3.3 Overview

A cohort of 10 high school educators from the Southwest Missouri region was carefully selected. Following an introductory week of foundational lessons, it became apparent that two educators from this group exhibited remarkable interest and enthusiasm towards the subject of IoT security vulnerabilities. Subsequently, over a span of five weeks following the initial week, these two educators, in collaboration with the support of faculty members and graduate mentors, dedicated themselves tirelessly to delving deeper into the intricacies of IoT security vulnerabilities. The methodology detailed in subsection 3.2 was rigorously adhered to throughout this period of intensive training and research.

Upon culmination of this rigorous training and research endeavor, the educators presented their findings and insights gleaned from this experience during the conclusion of the training program. Additionally, they consistently submitted comprehensive reports detailing their implementations of acquired knowledge within their respective school environments across various academic semesters.

4 Expected Outcomes & Preliminary Results

4.1 Curriculum Design

Following the completion of our research training focusing on security vulnerabilities in IoT devices, educators gained a comprehensive understanding of significant security gaps inherent in these devices. This knowledge empowered them to effectively impart this critical information to students through developing course materials, thereby enabling students to augment their understanding and undertake initiatives to address security vulnerabilities in IoT devices. As an outcome of our research training program, educators were tasked with formulating a curriculum outlining their preferred teaching approach. “Fig 2" illustrates the course plan devised by educators delineating their instructional strategies for educating students on IoT security.

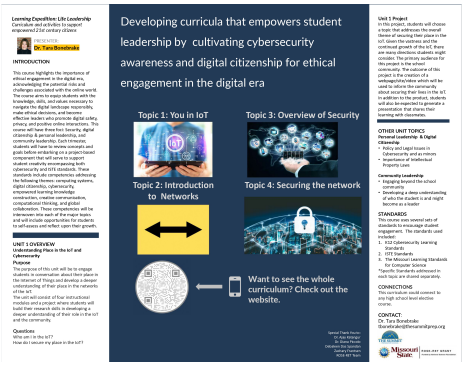


Fig. 2: Curriculum Design for IoT Security Learning

The course plan is structured around four distinct topics aimed at providing a comprehensive understanding of Internet of Things (IoT) and network security principles:

1. **You and IoT:** This initial topic focuses on elucidating the concept of IoT and identifying common smart devices encountered in daily life. The instructor aims to establish a connection between students' everyday experiences and the realm of IoT devices.
2. **Introduction to Networks:** Here, the instructors delve deeper into networking fundamentals, facilitating a nuanced comprehension among students. Practical exercises such as pinging a known IP address and conducting a Traceroute are employed to enhance understanding of network dynamics. The session includes illustrating connections between students, networks, and IoT devices through diagrammatic representations. Ethical considerations regarding network analysis are also discussed.
3. **Overview of Security:** This segment entails an explanation of the interactions within the Confidentiality, Integrity, and Availability (CIA) triad concerning data states. A strategic plan for implementing security measures to safeguard data across these states is formulated.
4. **Securing the Network:** The concluding segment focuses on addressing vulnerabilities inherent in IoT devices. Various types of attacks impacting information security for individuals and organizations are delineated. The session involves analyzing a network threat and proposing defense strategies. Interaction with students to gather insights aids in gauging their learning curve regarding IoT device security vulnerabilities.

Table 1 details the activities and tasks outlined for individual topics. These activities and tasks have been developed by educators with careful consideration of students' capabilities and the technologically advanced school smart environment prevalent in Southeast Missouri. Each topic within the curriculum has been meticulously crafted to furnish students with a comprehensive comprehension of

IoT concepts, network dynamics, security principles, and strategies for addressing cybersecurity challenges within an interconnected context. The design of these topics facilitates effective interaction among students, teachers, and smart IoT devices within the school premises.

4.2 Project Design

In crafting the project for our students, we focused on a theme that underscored the imperative of securing our position within the IoT landscape. Given the expansive nature and continual expansion of the IoT realm, numerous avenues are available for exploration. The primary target audience for this project encompassed the school community. The anticipated deliverable from this endeavor was the development of a webpage, site, or video that serves as an educational resource for the community, imparting knowledge on how to enhance security within their IoT-enabled environments. Additionally, a presentation was conducted to disseminate the acquired insights among peers within the class. "Fig 3" illustrates a sample IoT security project developed specifically for student engagement and learning.

Our overarching aim is to establish meaningful connections between the IoT, cybersecurity, and principles of leadership in everyday life. This holistic approach will not only deepen understanding of IoT security but also foster a sense of responsibility and empowerment within our community regarding their digital presence and safety.

Topic Considerations Students are encouraged to explore cybersecurity topics that hold relevance both in their personal lives and within the broader Summit community. Any subject pertaining to cybersecurity and students interest were taken into consideration for further investigation and analysis.

Analysis Students are required to conduct an in-depth analysis of a minimum of five scholarly sources pertinent to their selected topic. These sources were documented and shared on NoodleTools, accompanied by a concise annotation comprising two to three sentences. This rigorous approach ensured that students engaged with credible and diverse perspectives, thereby fostering a comprehensive understanding of their chosen subject matter.

Project Outcomes Students have endeavored to pinpoint a pertinent question or purpose pertaining to the selected topic. It is imperative for students to delineate relevant background information, particularly concerning threats and security issues. Our assessment encompassed an evaluation of each individual's stance concerning the topic within the IoT domain, as well as its implications within the classroom setting. The primary goal of this project is to facilitate the students' acquisition of a more profound comprehension of personal security within the context of the IoT.

Table 1: IoT Security Course Plan Developed by the Teachers

Topic	Activity	Tasks
You and IoT	Using video clips to discuss IoT.	Show clips from Mitchells vs. Machines
		Observations, thoughts, comments
		Discuss smart devices at home and School
	Visual assessment of school	Review observation protocol and observation document 5-10 minutes to walk around the school to look for and count smart devices
	History of IoT and Introduction to Networks	IoT History: https://youtu.be/DLH9p4vyvuM
		Introduction to LAN, WAN and Subnet: https://youtu.be/Fj02iTrWUx0
Introduction to Networks	Ethical considerations	When talking about cybersecurity and IoT, what do students already know?
		What are ethics? Why might it be important to understand ethics when considering cybersecurity?
		Ethical Hacking: https://youtu.be/XLvPpirlmEs
	Connecting to the Network	Parts of a network (short presentation)
		Send a Ping to a common IP address https://www.pagerduty.com/resources/ learn/ping-network-testing-connectivity/
		Trace Route https://www.educative.io/answers/ what-is-the-traceroute-tracert-command-and-how-is-it-used
	Fing/Nmap Activity	Show example of Nmap and Fing
		Topology and identification of devices in student home network
		Give task to create a map of the student's home network (identify the location and types of devices)
		Video Review of Nmap: https://youtu.be/wgNIva5nRjA
	Discussion	Why would mapping a network be helpful? Needed? (brainstorming and real life)
Overview of Security	Divide the students into Small Groups	Each group will become an expert in C, I, or A, and create a presentation that defines the data state and identifies at least one plan to protect that state of data.
		Complete a graphic organizer with the information.
	Discussion	Information security under threat in each of the three states
Securing the Network	Case Study: WannaCry Documentary	Watch the 30-minute documentary on YouTube https://youtu.be/PKHH_gvJ_hA
		Be prepared to discuss security issues and protections shared in the documentary.
	Assessing threats	How does the IoT increase potential threats to a person or a community?
		What do students think are the biggest threats to them (personally) in the IoT?
	Identifying defenses	Ways to defend against threats in the IoT?
		Research and share one method and the type of threat it can defend against

Project Critique Criteria Each iteration of the project underwent group assessment utilizing the creativity rubric, with group decision matrices done by other student groups. After the assessment, the scores were submitted to the instructor for evaluative feedback. Table 2 illustrates the creativity rubric utilized for evaluating student projects. The rubric delineates four key skills: Fluency, Flexibility, Originality, and Elaboration. Each criterion is assigned a score ranging from 1 to 4, with 1 representing a “Not so Great" performance and 4 indicating a “Great" performance, while scores of 3 and 4 denote “OK" and “Good" performances, respectively. Table 2 further explicates the definitions of each skill and outlines the methodology for score calculation. This structured approach ensured a comprehensive evaluation of student work, enabling targeted feedback and facilitating continuous improvement throughout the project cycles.

Table 2: Scoring Criteria for the Projects

Skills	Description	1 (Not So Great)	2 (OK)	3 (Good)	4 (Great)
Fluency	Have many ideas that could solve the problem	One or No appropriate Ideas	Few Appropriate Ideas	Some Appropriate ideas	Many Appropriate Ideas
Flexibility	All ideas are unique	One or two different kind of ideas or minor changes	Few different kind of ideas or minor changes	Some different kind of ideas or minor changes	Many different kinds of ideas or minor changes
Originality	Inspiration from existing ideas or completely new idea	Used other people ideas	Few original ideas	Some original ideas	Highly unique or unusual ideas
Elaboration	Detailed idea for building prototype	Very little description	Some details support the fact	Details used descriptive language	Well detailed and really paints picture

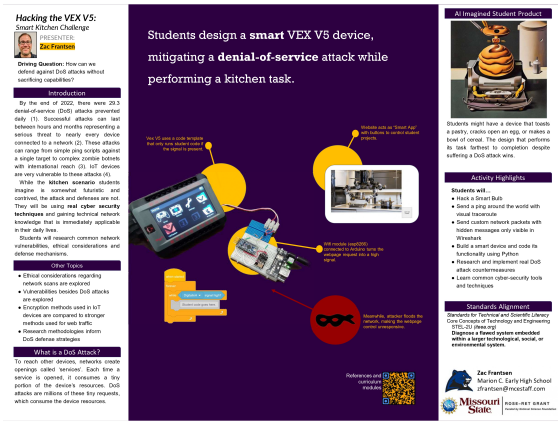


Fig. 3: Project Design for IoT Security Learning

4.3 Findings from Student Interaction Survey

The teacher training and research took place during the summer of 2023. Subsequent to the training, educators returned to their respective schools and incorporated their knowledge of IoT security vulnerabilities into their classroom curricula. This implementation occurred across two distinct courses offered at two different schools: Aerospace Engineering course at Marion C. Early High School and Expeditions: Life Leadership course at The Summit Preparatory School. Feedback from teachers indicated that students exhibited significant interest and enthusiasm for the subject matter, demonstrating a keen ability to grasp the concepts presented by their instructors. Classroom interactions were notably positive, reflecting a strong engagement with the training content. Additionally, we conducted an anonymous survey to gauge student interaction and participation within the classroom context, specifically concerning the topics covered in our training. Table 3 displays the questions utilized in our survey.

Table 3: Survey Questions

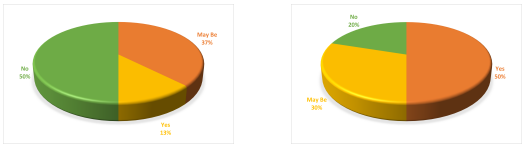
Survey Questions	Description	Options
SQ1	Are you aware of security vulnerabilities in IoT before this course?	1. Yes 2. No 3. May Be
SQ2	Are you aware of security vulnerabilities in IoT after this course?	1. Yes 2. No 3. May Be
SQ3	Will you be able to apply the learnings in your real life?	1. Yes 2. No 3. May Be
SQ4	Rate the contents of security in the curriculum	1-5

Figures 4, 5, and 6 depict the outcomes related to survey questions SQ1, SQ2, and SQ3. The analysis of “Fig 4" indicates that prior to the introduction of the IoT security content developed by the teachers at Marion C. Early High School, 50% of the students exhibited a lack of awareness regarding IoT security vulnerabilities. Conversely, at Summit Preparatory School, an equal percentage of students demonstrated awareness of these threats. However, the data presented in “Fig 5" reveals a significant increase in knowledge acquisition, with approximately 87% of Marion C. Early High School students and 90% of Summit Preparatory School students acquiring knowledge about IoT security threats through their recent coursework.

When evaluating students' confidence in implementing this knowledge in real-world scenarios, approximately 75% to 80% of students expressed full confidence in their understanding. Notably, while a minority of students may harbor less

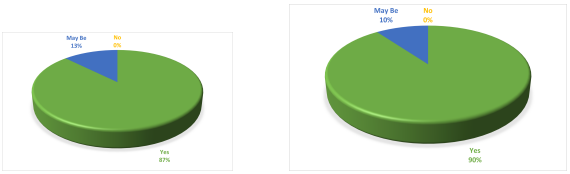
confidence in their knowledge, no students from either institution expressed outright negativity regarding their understanding of IoT security. This assertion is corroborated by “Fig 6", which provides supporting evidence for our claims.

In relation to SQ4 regarding content evaluation, a majority of students from both Marion C. Early High School and Summit Preparatory School provided ratings ranging from 3 to 5 on a 5-point scale. The mean student ratings were 4.25 and 4.00 for Marion C. Early High School and Summit Preparatory School, respectively.



(a) Marion C. Early High School (b) The Summit Preparatory School

Fig. 4: Students security knowledge before taking the course in the school

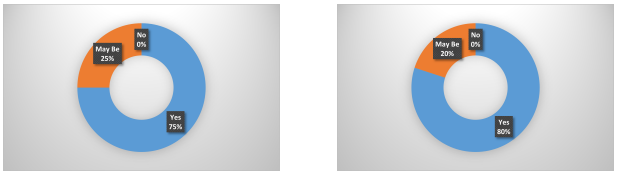


(a) Marion C. Early High School (b) The Summit Preparatory School

Fig. 5: Students security knowledge after taking the course in the school

5 Conclusion

The current state of professional development opportunities for high school teachers regarding security vulnerabilities within inclusive school environments is insufficient. Schools serve as foundational pillars for instilling societal and environmental awareness among students. Furthermore, schools house a plethora of smart IoT devices, making them ideal environments for fostering smart learning and environments. Therefore, equipping teachers with comprehensive knowledge of IoT devices and security vulnerabilities is essential for enhancing students' understanding.



(a) Marion C. Early High School

(b) The Summit Preparatory School

Fig. 6: Students security implementation ability after taking the course in the school

To address this need, we organized a summer training through the NSF RET grant program for high school teachers focused on IoT security vulnerabilities and defense strategies. Our objective was to empower teachers with the knowledge and research capability to educate students about security vulnerabilities associated with IoT devices in their surroundings. Additionally, indirectly through teacher training, we powered the teachers to inspire students in their classrooms to engage in further study and research in this domain, as well as instill a passion for computer science.

This paper outlines our training and research methodology in detail and evaluates the impact on teachers' learning, contributions, and outcomes through new curriculum and project designs. We also assessed student interaction and engagement with the developed content, noting their positive reception and increased interest. The innovative curriculum and projects developed by the teachers during their Summer experience have garnered favorable ratings from students and facilitated practical application of knowledge in real-world scenarios, even among those with limited prior exposure.

Moving forward, we intend to collaborate more closely with teachers and students in the SouthWest Missouri region to tailor content based on the student's interests. We will expand on defense strategies against security threats in school and home IoT devices, providing hands-on demonstrations for enhanced comprehension. Our goal is to cultivate a deeper interest among students through training the teachers with research capability and encouraging them to conduct independent research and self-study to identify and address security threats effectively.

Acknowledgments. This material is based upon work supported by the National Science Foundation under Award No. 2302060.

References

1. Ahmad Zukarnain, Z., Hashim, M.Z., Muhammad, N., Mansor, F.A., Wan Azib, W.N.H.: Impact of training on cybersecurity awareness. Gading Journal for Science and Technology **3**(1), 114–120 (2020)

2. Alam, T.: A reliable communication framework and its use in internet of things (iot). CSEIT **10**, 450–456 (2018)
3. Alkhalaf, S., Amasha, M., Al-Jarallah, A.: Using m-learning as an effective device in teaching and learning in higher education in saudi arabia. International Journal of Information and Education Technology **7**(6), 411–416 (2017)
4. Aspray, W., Aspray, W.: Recent efforts to broaden informal computer science education. Participation in Computing: The National Science Foundation's Expansionary Programs pp. 147–163 (2016)
5. Behera, S.K., Purulia, W.B.I.: M-learning: a new learning paradigm. International Journal on New Trends in Education and Their Implications **4**(2), 24–34 (2013)
6. Bernsteiner, R., Ebersberger, B., Kilian, D.: Mobile cloud computing for enterprise systems: A conceptual framework for research. International Journal of Interactive Mobile Technologies **10**(2) (2016)
7. Brown, T.H., Mbati, L.S.: Mobile learning: Moving past the myths and embracing the opportunities. International Review of Research in Open and Distributed Learning **16**(2), 115–135 (2015)
8. Bryan, L., Guzey, S.S.: K-12 stem education: An overview of perspectives and considerations. Hellenic Journal of STEM Education **1**(1), 5–15 (2020)
9. Chitanana, L., Govender, D.W.: Bandwidth management in the era of bring your own device. The Electronic Journal of Information Systems in Developing Countries **68**(1), 1–14 (2015)
10. Clay, I., Atkinson, R.D.: Wake up, america: China is overtaking the united states in innovation capacity (Apr 2023)
11. Custer, W.L.: Information security issues in higher education and institutional research. New Directions for Institutional Research **146**, 23–49 (2010)
12. Davies, R.S., West, R.E.: Technology integration in schools. Handbook of research on educational communications and technology pp. 841–853 (2014)
13. Deffree, S.: Engineering the next generation of stem. EDN-Electronic Design News **57**(5), 26 (2012)
14. Dlodlo, N.: The internet of things technologies in teaching, learning and basic education management. In: Southern African Computer Lecturers Association 2012 (SACLA 2012) (2012)
15. Elliott, C.: Botnets: To what extent are they a threat to information security? Information security technical report **15**(3), 79–103 (2010)
16. Escortell, R., Delgado, B., Martínez-Monteagudo, M.C.: Cybervictimization, self-concept, aggressiveness, and school anxiety in school children: A structural equations analysis. International Journal of Environmental Research and Public Health **17**(19), 7000 (2020)
17. Gereffi, G., Wadhwa, V., Rissing, B., Ong, R.: Getting the numbers right: International engineering education in the united states, china, and india. Journal of Engineering Education **97**(1), 13–25 (2008)
18. Goode, J., Margolis, J., Chapman, G.: Curriculum is not enough: The educational theory and research foundation of the exploring computer science professional development model. In: Proceedings of the 45th ACM technical symposium on Computer science education. pp. 493–498 (2014)
19. Green, S.L., Anid, N.M.: Training k-12 teachers in stem education: A multidisciplinary approach. In: 2013 IEEE Integrated STEM Education Conference (ISEC). pp. 1–4. IEEE (2013)
20. Hassan, I.: Teaching cybersecurity to computer science students utilizing terminal sessions recording software as a pedagogical tool. In: 2020 IEEE Frontiers in Education Conference (FIE). pp. 1–8. IEEE (2020)

21. Katehi, L., Pearson, G., Feder, M.: The status and nature of k-12 engineering education in the united states. The Bridge **39**(3), 5–10 (2009)
22. Lee, I., Lee, K.: The internet of things (iot): Applications, investments, and challenges for enterprises. Business horizons **58**(4), 431–440 (2015)
23. Mahamad, S., Ibrahim, M.N., Taib, S.M.: M-learning: A new paradigm of learning mathematics in malaysia. arXiv preprint arXiv:1009.1170 (2010)
24. Maqsood, S., Chiasson, S.: Design, development, and evaluation of a cybersecurity, privacy, and digital literacy game for tweens. ACM Transactions on Privacy and Security (TOPS) **24**(4), 1–37 (2021)
25. Martin, R., McGill, T., Sudweeks, F.: Learning anywhere, anytime: student motivators for m-learning. In: Proceedings of the Informing Science and Information Technology Education Conference. pp. 51–67. Informing Science Institute (2013)
26. Moreira, F., Ferreira, M.J., Santos, C.P., Durão, N.: Evolution and use of mobile devices in higher education: A case study in portuguese higher education institutions between 2009/2010 and 2014/2015. Telematics and Informatics **34**(6), 838–852 (2017)
27. Padilha França, R., Borges Monteiro, A.C., Arthur, R., Iano, Y.: An overview of internet of things security from a modern perspective. In: Brazilian Technology Symposium. pp. 639–652. Springer (2019)
28. Quayyum, F.: Cyber security education for children through gamification: Challenges and research perspectives. In: Methodologies and Intelligent Systems for Technology Enhanced Learning, 10th International Conference. Workshops: Volume 2. pp. 258–263. Springer (2021)
29. Rajasingham, L., et al.: Will mobile learning bring a paradigm shift in higher education? Education Research International **2011** (2011)
30. Samples, Q., Roque, L., Danielson, S., Mortenson, A., Gorski, D., Hinman, L., Collins, N., Walls, M., Hardaway, J., English, D.: What are the basic elements of iot (Dec 2023), `https://robots.net/tech/what-are-the-basic-elements-of-iot/`
31. Snyder, T.D., Dillow, S.A.: Digest of education statistics, 2011. nces 2012-001. National Center for Education Statistics (2012)
32. Snyman, D.P., Drevin, G.R., Kruger, H.A., Drevin, L., Allers, J.: A wolf, hyena, and fox game to raise cybersecurity awareness among pre-school children. In: International Symposium on Human Aspects of Information Security and Assurance. pp. 91–101. Springer (2021)
33. Tsinakos, A.: State of mobile learning around the world. Global mobile learning implementations and trends pp. 4–44 (2013)
34. Tyler, K., Abilkasimov, M., Grieveson, T.: Cyber risk management solutions, `https://www.bitsight.com/`
35. University, S.: How technology is reinventing k-12 education (Feb 2024), `https://news.stanford.edu/report/2024/02/14/technology-in-education/`
36. Vailshery, L.S.: Iot devices installed base worldwide 2015-2025 (Nov 2016), `https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/`
37. Van Mechelen, M., Smith, R.C., Schaper, M.M., Tamashiro, M., Bilstrup, K.E., Lunding, M., Graves Petersen, M., Sejer Iversen, O.: Emerging technologies in k–12 education: A future hci research agenda. ACM Transactions on Computer-Human Interaction **30**(3), 1–40 (2023)
38. Wang, E.K., Ye, Y., Xu, X., Yiu, S.M., Hui, L.C.K., Chow, K.P.: Security issues and challenges for cyber physical system. In: 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing. pp. 733–738. IEEE (2010)