A three-year retrospective on offering an embedded systems course with a focus on cybersecurity

A. Ravishankar Rao, PhD,
Fellow, IEEE
Fairleigh Dickinson University, NJ, USA
raviraodr@gmail.com

Abstract

The fast pace of advancement in fields of computer science and engineering creates enormous opportunities for the use and application of computing devices. The internet of things (IoT) constitutes an area experiencing significant growth. If IoT systems are not configured and used correctly, there is potential for widespread disruption and harm due to cyberattacks. Hence, the new generation of professionals in the field of computer technology needs to be conversant with cybersecurity and the design of protection of computer systems.

Cybersecurity is not restricted to a specific domain such as hardware or software and needs to address all aspects of operation of computer systems. Consequently, we have found it beneficial to introduce students to cybersecurity through an embedded systems course. Based on three years of teaching cybersecurity to students in an embedded systems course, we observe that students are excited and motivated to participate in hands-on lab exercises. We have taken special care to orient these lab exercises to breaking news articles about developments related to safety and cybersecurity. We also found it helpful to unify multiple lab exercises around a specific target application domain such as healthcare or retail.

Our results over a three-year period demonstrate that it is possible to teach essential cybersecurity concepts within a one-semester course to students who do not have prior exposure to this area. This knowledge needs to be expanded upon in other courses, thereby weaving a thread of cybersecurity through the students' educational experience.

Index Terms – embedded systems, curricular development, hands-on experience, internet-of-things, databases

INTRODUCTION AND MOTIVATION

There is growing concern about the decline of science and engineering capacity in the U.S. [1]. For instance, the number of U.S. full-time graduate students in electrical engineering declined by 17% from 1995 to 2015. Despite billions of dollars spent on high school programs, student performance has stagnated over the past decade [2].

On the other hand, the number of foreign students has risen substantially and many of them have been employed by the growing technology industry in the U.S. However, there is concern regarding a shortfall in candidates for critical jobs in the U.S. government sector requiring security clearance including defense and national security [3]. The demographic picture is not encouraging either, as many colleges are experiencing declining student enrolments [4].

Hence it is imperative for educators and educational institutions to seek innovative approaches to attract students to STEM fields, retain them and improve the quality of STEM education. There are a growing number of non-profit organizations like Girls-who-code that promote STEM careers to women (https://girlswhocode.com). Simple interventions such as using elements from the arts and cinema are helpful in improving student motivation [5, 6]. Classroom attention and engagement can be enhanced by nudging students away from cellphone use during classes [7].

Traditional lecture formats may not appeal to the younger generation of students [8]. The use of a greater number of hands-on laboratory exercises makes students more interested in the subject matter [9-11]. We have used this approach steadily over the past three years by continuously modifying an existing course on embedded systems. This course is taught to both graduates and senior level undergraduates at Fairleigh Dickinson University (FDU). We describe our strategy, approach and lessons learned. This experience will be helpful for instructors across the spectrum, from high school to the graduate level at universities.

Specifically, we present our design of an Internet-of-things (IoT) lab using a Raspberry-Pi computing platform with multiple peripheral devices. We explore the target application domains of healthcare and retail. We weave a thread of cybersecurity throughout the course as this is an area of growing concern due to the potential for cyberattacks through IoT devices. It is helpful to repeat the theme of cybersecurity in multiple related lab exercises as it fosters a "security mindset" [12] in the students. We are developing a similar set of hands-on laboratory exercises in data science to students in another course in order to develop a "data habit of mind" [11].

BACKGROUND

Many hardware components have fallen drastically in price and are widely available. The website adafruit.com offers nearly 200 different sensors which can be utilized through inexpensive computing platforms such as the Raspberry-Pi and Arduino. Interesting application domains include environment monitoring, digital health and home automation. Depending on the ability of the student, exciting projects can be created from the high school level to the graduate level in universities. Many commercially systems are available including the Nest smart thermostat and the Ring doorbell with integrated cameras. It is possible to create such systems from scratch using off-the-shelf components. Engaging in such creation teaches students important design, implementation and debugging skills.

Software components are also becoming increasingly open source and free. Due to websites such as github.com, it is relatively straightforward to download and configure software components. Making the hardware and software work together is still challenging due to factors such as the version level of the software components, compatibility of device drivers and wiring issues with the devices.

Jang et al. [13] contrast trends related to IoT education at the K-12 level in the US, UK and Korea. The Korean ministry of education in 2015 introduced an informatics curriculum which explicitly includes IoT education. In the US, the 2016 K-12 computer science framework does not mention IoT. Similarly, the computing education curriculum in the UK in 2014 does not explicitly discuss IoT. Nevertheless, the computing curricula are moving in the direction of understanding physical computing systems and the interaction between computing systems and the physical world. Though there are efforts by educators to create IoT courseware [13, 14], there is no explicit focus on cybersecurity issues.

Cybersecurity is becoming an important consideration in the use and deployment of IoT devices. Since IoT devices are cheap and widely deployed, the large attack surface that can be exploited is increasing. Due to their low cost, manufacturers are reluctant to add extra features related to security. Users are either unaware about configuring the devices to protect themselves, or find the process cumbersome.

The author has been fortunate to receive two separate grants from the National Security Agency in the US to set up an IoT lab to explore embedded systems security. The first grant was executed during 2017-2019 and the second grant is for the 2019-2020 period. The goal of this ongoing effort is to design, implement and test hands-on lab exercises that develop student understanding and competence in security issues. The know-how includes detailed instructions on preparing each lab, a parts list, software components, code and material for use by educators. In the current paper, we summarize our approach to designing these labs and the experience of students while carrying out the labs. (Details may be found in [9, 10, 15]). There is always scope for improvement, and a community-wide effort is required where instructors can share their experience and learn collectively. This will enhance the overall quality of courseware.

Requirements

The existing Embedded systems course at Fairleigh Dickinson University (FDU), EENG7709, is taught by the author at the graduate level. This combines instruction in hardware and software, and considers inexpensive computing devices used in control applications and many consumer gadgets. Due to the recent explosion of the internet-of-things, this has become an important course. Based on our experience in teaching this course from 2015-2016, we formulate the following requirements for introducing cybersecurity content into such a course.

1. The course should appeal to students from a wide range of backgrounds, including bachelors vs. masters level, electrical engineering vs. computer science, and domestic vs. foreign students.
2. Students may not be able to come to the laboratory outside the assigned contact hours for the class.
3. The new content must fit into an existing course taught over one semester, with 15 weeks of lectures at 2.5 hours per lecture.
4. No prior background in cybersecurity should be assumed.
5. The devices used should be inexpensive, standardized and readily available.
6. The devices should not require special clearance, and should be usable by all students.
7. The devices should be isolated from regular computer networks.
8. Different laboratory exercises should be unified through a common theme, such as a target application domain.
9. Meaningful lab exercises should be designed to relate them to real-world applications and capture the students' interest.
10. A methodology for continuous improvement and updating needs to be established.

We analyze our proposed method to meet these requirements in the next section. Our rationale will help other instructors design similar courseware along these lines.

METHODS

We first analyze the requirements laid out earlier and present our approach to satisfying them.

1. The wide background of students poses a significant challenge. Many electrical engineers do not have sufficient exposure to programming, especially the foreign students. Similarly, students in computer

science have limited exposure to hardware and interfacing with devices. Few students have prior exposure to the desirable skills in embedded systems programming which includes Python and Linux today. Consequently, we devoted the first half of the course to teaching basic Python and Linux programming skills. This was done in addition to the regular course material for embedded systems. Students were assigned an online interactive textbook from zybooks.com for learning Python. This accelerated their learning.

2. Most students are commuters at our campus. Several have full-time jobs and can be on campus only for the duration of the lecture. Though the technology lab facilities for the course are kept open until 10pm on weekdays and until 5pm on weekends, most students are not able to utilize the equipment outside class hours. Furthermore, students cannot complete the lab work at home, as they need to have the necessary equipment. Hence, it is necessary for the lab to be structured so that students can finish it during the allotted instruction time of 2.5 hours. It is also not possible to mandate an extra session for laboratory work due to scheduling constraints. An alternate approach would be to loan the necessary equipment to the students so that they can take it home for the duration of the course. Students could also be required to purchase the equipment. This creates challenges of its own, such as maintenance and updates.
3. We structured the course so that lectures in the second half of the course contained one hour of instruction followed by 1.5 hours of laboratory work. This made the modules self-contained. Students were able to finish the required work and take the appropriate measurements. They completed their lab reports at home.
4. No prior background in cybersecurity was assumed. The embedded systems course is a good launching pad for introducing cybersecurity as there are many potential vulnerabilities in embedded devices. We chose the Raspberry Pi computing platform to teach cybersecurity skills due to its low cost and customizability. Students could quickly learn the basics of computer networking, including the creation and use of firewalls. These topics can be introduced efficiently within a single lecture and lab session.
5. In addition to the Raspberry Pi, we used multiple low-cost sensors that interface readily with the Raspberry Pi. A few of them including barcode scanners are described in more detail in the following section.
6. We did not use devices that require FCC clearance, medical clearance or had any safety issues.
7. The advantage of using the Raspberry Pi is that it can be used to create a stand-alone computer network that is isolated from the regular university network. Hence, any student errors will not cause any outage of the regular networks.
8. We selected the themes of healthcare and retail in order to integrate the different lab exercises. Student gain a better understanding of an application domain by considering multiple devices that are used within a common framework. If properly designed, there is sufficient time to explore one or two such application domains within a one semester course.
9. The lab exercises were made relevant to real life scenarios by connecting them to recent developments reported in the press. Due to the increasing usage of IoT devices and the overall lack of security measures, the number of cyber-attacks has also been increasing. Many of these incidents are receiving news coverage and analysis, and raise important issues and concerns that must be addressed by the technical community.
10. We have started using short questionnaires at the end of every lab. Students are asked to note down the time it took to complete the lab and prepare their reports. This serves to calibrate and adjust the workload so it can be realistically completed by the students in the allotted time. Furthermore, students are also asked to report areas in which they faced problems and how that could be addressed in the future. This continuous feedback provided by students throughout the course is far better than the traditional end-of-semester course surveys carried out by most universities. Students simply don't have the time at the end of the semester to provide meaningful feedback as they are rushing to complete all their assignments and to prepare for final examinations.

Student demographics

The size and composition of the classes over the three years is reported in Table 1. The course is becoming attractive to students who are signing up for the integrated 5-year Bachelor's/Master's degree program being offered at FDU. Hence, some undergraduate students are taking this course in their senior (fourth) year of studies. The background of the students consists of a mix of electrical engineering, computer engineering and computer science. There are more foreign students than domestic students, which is typical of graduate courses in engineering across U.S. universities. We had to accommodate the diversity of student backgrounds in designing the course material.

	Fall 2017	Fall 2018	Fall 2019
Class size	8	11	12
Undergraduates	0	4	5
Graduate students	8	7	7
Electrical Engineering	7	9	9
Computer Engineering/Computer Science	1	2	3
Domestic students	1	5	5
Foreign students	7	6	7
Males	4	6	7
Females	4	5	5

Table 1: The composition of students in each class.

Design of Lab Modules

Based on the above requirements, we have designed the following sequence of lab modules that combine essential aspects of embedded systems with exposure to basic cybersecurity concepts. Several of these labs are described in detail and are uploaded to the website provided by the National Security Agency for dissemination to the wider public [16]. The uploaded material is suitable for use by instructors at other institutions and students interested in self-study. Each lab is self-contained, and provides a list of necessary hardware and software components. The software is either publicly availabe and free such as the Raspbian operating system, or has been written by the author and his students and made available through the GPL Gnu Public License. This allows the community to use existing material efficiently.

Lab 0: Introduction to the Raspberry-Pi.
Lab 1: Network configuration
Lab 2: Using Raspberry-Pi for distributed temperature sensing
Lab 3: Understanding random number generation.
Lab 4: Simulating a dictionary attack
Lab 5: Automatic Update of Firewall Rules
Lab 6: Simulating a SQL Injection attack

These labs were offered and tested during the Fall 2017 and Fall 2018 semesters. These labs are very general and are applicable to any domain where embedded systems are in use. In order to give students more depth in understanding the applications of embedded systems, it is necessary to cover the needs of specific domains. Hence we started creating additional lab exercises that are specific to the target domains of healthcare and retail. These two domains are witnessing impressive growth in the use of embedded devices for functions such as patient monitoring, digital health and tracking shipments including medical supplies. There are many unsolved problems in these domains. Hence the imagination and creativity of a younger generation of workers is necessary to create successful systems of the future. By introducing these domains, application scenarios and existing problems to the students before they graduate, we give them more time to consider ideas and potential solutions. They may even spur the creation of startups, which is becoming increasingly common at university campuses, especially in the US.

Based on these observations, we created a new set of lab exercises for the Fall 2019 semester, listed below.

Lab 7: Using barcodes to tag medical devices
Lab 8: Using biometrics for patient identification
Lab 9: Using sensors to measure patient vitals

These labs are focused on embedded systems applications that are becoming more relevant in hospitals. We briefly describe the lab material, results and student reactions for Labs 7-8 in this paper. Further technical details may be found in [17].

Lab 7: Using barcodes

The use of barcodes has revolutionized many industries such as shipping and retail. The availability of cheap barcode scanners and software that processes this data is transforming the retail industry. It is common to find several self-checkout lanes in supermarkets these days, where even novice users of this technology are able to proceed without problems. Hospitals are also introducing barcode technology in multiple areas including tracking shipments, tagging equipment and identifying patients. Barcodes help to ensure the safety and security of medical devices and medications through the reduction of counterfeiting. Hence, the introduction of barcode scanners is a natural choice for an embedded systems course.

Though one may expect that this technology works flawlessly, there are several practical challenges in deploying it. Sometimes barcode scanners may produce errors, or certain barcodes may not be easy to read, for instance from curved surfaces such as a wristband. Such difficulties were reported recently in a New York Times article written by a healthcare provider [18]. This creates an interesting exercise for the students, who can verify whether such reported observations can actually be replicated. This exercise shows students the value of staying in touch with the news and real-world developments. They come to realize that these classroom exercises are not merely hypothetical but intimately connected with practical applications.

Figure 1 depicts the setup of the lab experiment and a wristband that simulates a patient identification bracelet.

(A): Schematic showing the devices used.

(B): A printed barcode worn as a wristband. This simulates a patient identification wristband that could be used in hospitals.

Figure 1: Describes the setup and use of materials in the lab for barcode scanners.

Lab 8: Using fingerprint sensors for patient biometrics

Fingerprint readers are also becoming popular due to their low cost and reasonably accurate operation. Many mobile phones now offer fingerprint readers to unlock the device. The use of biometric information provides an alternate method to identify a person, apart from the usual methods such as name, date of birth, driver's license and passport. In hospitals, patients are typically identified by their name and date of birth rather than biometrics. This is due to multiple factors, including the cost of deploying biometric technology and the reluctance of some patients towards providing biometric information. Nevertheless, biometric technology can potentially avoid misidentification of patients in hospitals. A recent article in the Wall Street Journal pointed out current limitations with using just the name and date of birth for patient identification, which leads to occasional errors [19]. The implications of patient misidentification are extremely serious, and we need to explore better methods that work in practice.

Figure 2 shows a fingerprint sensor used by students in our lab. The students first learn how to wire the device correctly. Then they learn how to install and use the software to operate the sensor. Finally, they learn how to interpret the results for the usage of the device in practical applications. Some exercises conducted by the students included rotating the finger by varying amounts while it is placed on the scanner, and exploring how clean the surface of the sensor needs to be.

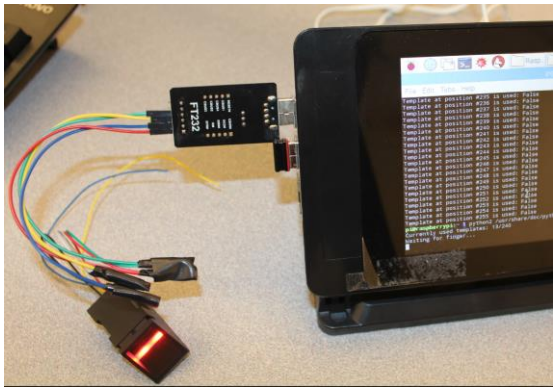

Figure 2: Shows a fingerprint sensor connected to the USB port of a Raspberry-Pi machine in our lab.

Lab 9: Using a pulse sensor to record patient vitals

Though cheap digital sensors are available for many measurements, healthcare providers manually enter several variables related to patient vitals into a computer. There is potential for human error in these situations. The accuracy of patient records could be improved by recording information directly from the measuring device.

In this lab, we introduced an inexpensive pulse sensor that can be connected to the Raspberry Pi as shown in Figure 3.

Figure 3: We used a pulse sensor (made by pulsesensor.com) and connected it to the Raspberry Pi. With software from this website students were able to obtain their pulse readings and record it automatically into a database.

RESULTS

Lab 7: Using barcodes

All 12 students in the Fall 2019 class reported that they found the lab interesting and that this lab taught them several practical skills. Some of their responses are recorded below. Several students did not know SQL (Structured Query Language), which forms the backbone of database technology. Hence, this lab was also able to give the students an introduction to SQL in a short period of time.

Students had full control of the software and could modify at as desired. The software was written in Python and runs on Linux. Both are open source and free.

A few student reactions to the lab are noted below.

> It was very useful to have such labs with such implementation. I now have broad vision in how we can integrate any device with Raspberry Pi and use the whole as a one device that can benefit us in many ways.
>
> The interactions between hardware and software I find very interesting as I learned in few courses about SQL and different data bases but never had it implemented in something this close to daily life.
>
> I learned how Python can be used to work with a SQL database, and how powerful the combinations of the two tools are.

Lab 8: Using fingerprint sensors for patient biometrics

All 12 students in Fall 2019 were pleased to learn a new skill and found the lab interesting. Sample student responses are shown below. These results demonstrate that students enjoy exploring such systems and finding answers to questions. Once they understand the working of these systems, they are confident about carrying this knowledge forward to practical situations. Sample student reactions are shown below.

> I now understand how to use a fingerprint reader with the Raspberry Pi and how to apply this in retail and healthcare domains.
>
> Navigating the Raspberry Pi is new to me, so working with it is still fascinating. Additionally, working on the fingerprint scanner and trying to get different configurations to work was fun.

Lab 9: Using a pulse sensor to record patient vitals

All 12 students in Fall 2019 completed this lab during the allotted time and found it interesting. Sample responses are reported below. Note that students are able to connect these lab exercises to the working of everyday devices they have grown accustomed to in their daily life. By understanding all aspects of the systems, from hardware through software to usage, they are better able to grasp potential security issues.

> This lab was interesting as it covers some information about heartbeats sensors. Heartbeats sensors are everywhere nowadays and most companies have attached this technology to the products they make.
>
> This lab helps me understand the pulse sensor applications of embedded systems. The sensor used in this lab looks like the sensor in my smart band. Hence, through this lab, I can easily learn about the theory about the pulse sensor and implement it.

One of the lectures covered the topic of SQL injection, which is a way for attackers to hack into a system through security vulnerabilities in SQL. Since the students had already used SQL in the previous labs, they were better able to understand the different entry points for attackers through such IoT devices.

DISCUSSION

The use of embedded devices and automatic monitoring systems in vehicles and aircrafts is increasing dramatically. In some instances, their malfunction has led to serious investigations with global consequences. The fuel emissions control system in Volkswagen vehicles was configured to fraudulently evade emission laws. A recent article in IEEE Security and Privacy discusses ethical violations [20] that led to the Dieselgate scandal. The tragic Boeing 737 MAX crashes illustrate the challenges of designing safety-critical software systems that receive sensory input. The interpretation of sensory signals is key to ensuring the safety and security of the aircraft [20]. These cases were also discussed during the embedded systems class, and serve as a bridge between classroom material and the real world. Due to their complexity, many issues are intertwined, ranging from the engineering aspects of the system to management and ethical lapses.

In the realm of cybersecurity, recent developments include ransomware attacks on city governments and hospitals. Coincidentally, a local hospital in New Jersey was the victim of a ransomware attack [21] during the last week of the Fall 2019 semester. Students were asked about steps that could be taken to prevent such attacks. Due to their exposure to cybersecurity concepts during the course and a focus on the

healthcare industry, students gave knowledgeable and relevant answers. They realized that concepts learnt in the course are not merely theoretical, but can be applied readily to real-life situations unfolding on a daily basis.

The increasing frequency of ransomware attacks is also raising several ethical issues. One issue is whether victims should pay the ransom. On the one hand, paying the ransom would serve to encourage criminals to continue their attacks. Thus, affected organizations should refrain from paying the ransom and fix their own systems. On the other hand, it may be far more expensive and time consuming to restore computer operations to working order than pay the ransom. In certain critical situations like hospital environments, it is imperative that systems be restored as quickly as possible, which necessitates the paying of the ransom. The discussion of these issues provides STEM students a well-rounded perspective on the totality of engineering and information-technology systems. Sound decisions need to be made at all levels, starting at the device level and proceeding to the system, organizational and societal levels.

The processing power of many IoT devices is steadily increasing. This is spurring the development of new applications, sometimes even by creators who are not experts in technology. For instance, a student at New York University with a background in journalism founded the company gotenna.com, which uses radio antenna attached to Raspberry Pi machines to create off-grid communication networks. This is a welcome development, as the US needs to get more students involved in computer hardware and manufacturing.

The New Lab (newlab.com) that opened recently in Brooklyn, NY is an innovation and prototyping hub that has several startups working on IoT technologies. A recent article expressed surprise at the growing number of manufacturing companies within New York City working on applications such as underwater drones and traffic monitoring systems[22].

The significant loss of manufacturing jobs in the U.S. was a central theme in the US presidential elections of 2016. Nimble companies that focus on emerging technologies such as IoT and automation may be a possible solution to reverse this situation. By connecting students with the local technology ecosystem, we can expect further growth and investment in IoT technologies within the U.S. Students in the embedded systems course were made aware of these types of opportunities.

CONCLUSION

We reviewed the design and implementation of hands-on lab exercises to teach students about the cybersecurity of embedded devices. Since the use of such devices is growing rapidly, it is important to educate the current generation of students about their safety and security aspects. We found that lab exercises designed around a specific application domain such as healthcare or retail provided a consistent theme across multiple lectures. By exploring the configuration and use of different sensors, students were stimulated to conduct their own experiments and think of different applications. We also included an investigation of recent news articles that reported problems in the use of these sensor technologies in real-world settings. Such an exercise helps the students develop a balanced outlook, where the excitement of new technologies is tempered with the caution regarding potential pitfalls. The net result of such an educational approach is to prepare mature and capable practitioners.

ACKNOWLEDGMENTS

The Raspberry-Pi equipment bought for this project was supported by the National Security Agency (NSA) under Grant/Cooperative Agreement entitled ‘Cybersecurity Workforce Education - CNAP Initiatives’ Number H98230- I 7- I -032 I. Specifically, the following grant was awarded to Fairleigh Dickinson University: “*Developing Hands-on Exercises for Secure Embedded System Design & Security Data Analytics for Computing and Engineering Students.*”, *CNAP-CAE CNAP-CAE2017 Grant# H98230-17-1-0321*.

The project was also supported by the National Security Agency under Grant/Cooperative Agreement Fairleigh Dickinson University CySP Grant Number H98230-19-1-0272. The United States Government is authorized to reproduce and distribute reprints not-withstanding any copyright notation herein.

AUTHOR INFORMATION

A. Ravishankar Rao is an Assistant Professor of Computer Science and Engineering at Fairleigh Dickinson University. He teaches graduate as well as undergraduate courses. He conducts research in computational neuroscience, big-data analytics, embedded systems, cybersecurity and STEM education. He is an Associate Editor of the journals Pattern Recognition and Machine Vision and Applications.

REFERENCES

[1] E. R. Dougherty, "The Decline of American Science and Engineering," *American Affairs*, vol. 3, 2019.

[2] E. Richards, "Despite Common Core and more testing, reading and math scores haven't budged in a decade," in *USA Today*, ed, 2019.

[3] A. Herman, "America’s STEM Crisis Threatens Our National Security," *American Affairs*, vol. 3, 2019.

[4] N. D. Graw. (2019, Nov 1, 2019) The Enrollment Crash Goes Deeper Than Demographics. *Chronicle of Higher Education*.

[5] A. R. Rao, "A novel STEAM approach: Using cinematic meditation exercises to motivate students and predict performance in an engineering class," in *Integrated STEM Education Conference (ISEC), 2017 IEEE*, Princeton University, 2017, pp. 64-70.

[6] A. R. Rao, "Interventions for promoting student engagement and predicting performance in an introductory engineering class," *Advances in Engineering Education*, 2020.
[7] A. R. Rao, "Simultaneously educating students about the impact of cell phone usage while creating a metric to predict their performance," in *2018 IEEE Integrated STEM Education Conference (ISEC)*, 2018, pp. 143-148.
[8] V. Lakshminarayanan and A. C. McBride, "The use of high technology in STEM education," in *Education and Training in Optics and Photonics: ETOP 2015*, 2015, p. 12.
[9] A. R. Rao, D. Clarke, M. Bhadiyadra, and S. Phadke, "Development of an Embedded System Course to Teach the Internet-of-Things," in *IEEE STEM Education Conference, ISEC*, Princeton, 2018, pp. 154-160.
[10] A. R. Rao and R. Dave, "Developing hands-on laboratory exercises for teaching STEM students the internet-of-things, cloud computing and blockchain applications," in *IEEE Integrated STEM Education Conference*, Princeton, NJ, 2019.
[11] A. R. Rao, Y. Desai, and K. Mishra, "Data science education through education data: an end-to-end perspective " in *IEEE STEM Education Conference (ISEC)*, Princeton, 2019.
[12] S. Hooshangi, R. Weiss, and J. Cappos, "Can the security mindset make students better testers?," in *Proceedings of the 46th ACM Technical Symposium on Computer Science Education*, 2015, pp. 404-409.
[13] Y. Jang, J. Kim, and W. Lee, "Development and application of internet of things educational tool based on peer to peer network," *Peer-to-Peer Networking and Applications*, vol. 11, pp. 1217-1229, 2018.
[14] J. He, D. C.-T. Lo, Y. Xie, and J. Lartigue, "Integrating Internet of Things (IoT) into STEM undergraduate education: Case study of a modern technology infused courseware for embedded system course," in *2016 IEEE Frontiers in Education Conference (FIE)*, 2016, pp. 1-9.
[15] A. R. Rao and D. Clarke, "Capacity Building for a Cybersecurity Workforce Through Hands-on Labs for Internet-of-Things Security," in *National Cyber Summit*, 2019, pp. 14-29.
[16] M. Dark, S. Kaza, and B. Taylor, "{CLARK}–The Cybersecurity Labs and Resource Knowledge-base–A Living Digital Library," in *2018 {USENIX} Workshop on Advances in Security Education ({ASE} 18)*, 2018.
[17] A. R. Rao, N. Recharla, and K. Mishra, "Designing an internet-of-things laboratory with multiple sensors to improve student understanding of secure embedded systems," presented at the National Cyber Summit, 2020.
[18] T. Brown, "The American Medical System Is One Giant Workaround," in *New York Times*, ed, 2019.
[19] B. Gormley, "Hospitals Turn to Biometrics to Identify Patients," in *Wall Street Journal*, ed, 2019.
[20] R. L. Trope and E. K. Ressler, "Mettle fatigue: VW's single-point-of-failure ethics," *IEEE Security & Privacy*, vol. 14, pp. 12-30, 2016.
[21] M. Diamond, "Hackensack Meridian: We paid ransom to hackers to stop hospital cyber-attack," in *Asbury Park Press*, ed, 2019.
[22] C. Risen, "Underwater Drones, Mars Rover Parts and a High-Tech Revival," in *New York Times*, ed, 2019.