Towards Application-Driven IoT Education

Mounib Khanafer
American University of Kuwait
mkhanafer@auk.edu.kw

Tushar M. Jois
Johns Hopkins University
jois@cs.jhu.edu

***Abstract*—The increased popularity of Internet of Things (IoT) systems and platforms in various engineering and science fields has made training practitioners in IoT a necessity. At the same time, the active evolution of research on IoT has made available a wealth of educational resources like evaluation and development kits, web development frameworks, single-board microcontrollers and minicomputers, and hands-on books and courseware. The diversity of applications served by IoT from one side and the abundant educational resources from the other side raise questions on how best to train practitioners in IoT.**

In this paper, we introduce a new approach in designing and teaching a course on IoT: application-driven IoT education. The aim of this course design is to teach IoT through understanding a target application in depth. Rather than introducing IoT conceptually over several weeks before linking the theoretical concepts to an application, in an application-driven course the audience instead first learns a real-world application; then, students utilize the different components of an IoT platform (sensors, actuators, connectivity technologies, web interface, and cloud computing) to realize the application. To better demonstrate the concept, we use the application-driven approach to design a "smart home security and privacy" IoT course. This work is based on a combined experience of three years of teaching and researching IoT at both the American University of Kuwait and Johns Hopkins University.

I. Introduction

The Internet of Things (IoT) refers to a platform in which ordinary objects become *smart*: capable of connecting to the Internet to actively collect and exchange data. Equipped with sensing hardware, these smart things collect a massive amount of data from their surrounding environments. This data is further analyzed either locally or by a resourceful cloud server for an appropriate action to be taken by the actuator circuit connected to the IoT device [1].

IoT arose out of diverse research fields in electrical engineering and computer science. Examples of these fields include wireless sensor networks (WSNs), embedded systems, cloud computing, big data analytics, mobile computing, and communication protocols [2]. Consequently, a wide space of IoT applications was soon to emerge and cover various aspects of the modern life. Today, potential IoT applications include smart homes, smart cities, connected cars, traffic management, weather monitoring, smart grids, fleet tracking, body area networks, and wearable electronics [1], [3], all made possible with the interconnection of millions of intelligent objects [4].

As IoT technologies started to mature, many sectors and industries adopted IoT into their operations. The need for IoT-trained graduates increased, and universities worldwide started to scale up teaching IoT [5]. The community started to offer training courses on IoT for practitioners, with studies emerging that focused on IoT education opportunities and challenges [6]. With the growing interest in IoT, vendors worked on developing educational kits and single-board computers (SBCs) for prototyping and testing IoT systems [7]. Furthermore, programming languages (*e.g.*, Python, Java, and C), cloud services (*e.g.*, ThingSpeak, Google Cloud IoT, and Amazon AWS), and web development frameworks (*e.g.*, Django, Blynk, Cayenne, Flask, and MIT App Inventor) started to provide strong support to IoT design and implementation requirements. The rapid growth in the availability of educational resources, hands-on manuals, and specialized courseware for IoT led to a strong foundation for IoT education; several works focused on proposing designs or plans for teaching courses on IoT [1], [8], [9], [10].

With a close look at the available related literature, we can observe that the methodologies followed in teaching IoT courses are either lecture-based or project-based. In lecture-based learning, IoT is taught in the traditional way, *i.e.*, lectures, readings, and problem sets, just like any other topic in engineering or computing. In project-based learning, more emphasis is given to hands-on experience through practical assignments and team-based projects. To complement these methodologies, we state the following observations that motivate a new approach to tackle IoT education:

- IoT builds on skills in various topics including software development, hardware design, communication technologies, computer networking, cloud computing, web applications, and mobile computing. Expecting students to have accumulated knowledge in these topics before training them on IoT is a challenging task and maybe overwhelming for some students.
- A wealth of educational material, hands-on manuals, technologies, and tools are available for implementing the project component of an IoT course. Identifying which resources are more relevant to a specific domain or application may lead to more specialized IoT learning.
- As IoT systems are being developed and adopted by various industries, IoT courses can benefit from a more holistic design, incorporating ideas from subject matter experts in various fields.

With these observations in mind, we present in this paper the *application-driven* IoT education: a new approach to teach IoT that first highlights the application of interest and then shows how the requirements of this application can be fully

met and realized through one of the available IoT architectures. This approach of teaching is advantageous as it achieves the following:

- Learners are better engaged, as the course focuses on an immediately-relevant, practical application.
- The educator can make informed selections of the tools to introduce for hands-on learning.
- The prerequisites for such a course are narrowed down to meet the scope of the application, broadening the pool of potential students.
- The course can be further specialized for subsequent classes in a sequence by studying additional applications (*e.g.*, from a first-year smart home IoT course to a second-year autonomous car IoT or healthcare IoT course).
- Experts from different fields who have interest in the same application can collaborate to create interdisciplinary courses, and spur new research directions in IoT.

Our contribution in this paper is twofold:

1) We introduce a new approach to teach IoT for engineering and computing students named *application-driven* IoT education.
2) We provide an example on how to implement this new approach to design an IoT course driven by *security and privacy in smart homes*.

It is worth mentioning that this work draws from experience in teaching and researching IoT for three years at the American University of Kuwait and Johns Hopkins University [8], [1], [11].

The rest of the paper is organized as follows. Section II provides a formal definition of IoT and its architecture. Then, Section III provides background on the related work. Next, Section IV describes the new concept of application-driven IoT education and how to design an IoT course based on it. After that, Section V presents an example on how to apply the application-driven IoT approach in designing a course driven by security and privacy in smart homes. Finally, Section VI concludes this work.

II. IoT Definition and Architecture

The IoT European Research Cluster (IERC) [12] defines the Internet of Things as follows:

> *"A dynamic global network infrastructure with self-configuring capabilities based on standard and inter-operable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network."*

The authors in [2] have used this definition to delineate the following components of an IoT system:

1) **IoT devices**: The resource-constrained smart things that collect data and perform actions in an environment.
2) **Cloud servers**: The relatively-powerful remote cloud servers that conduct data analysis and store data in databases.

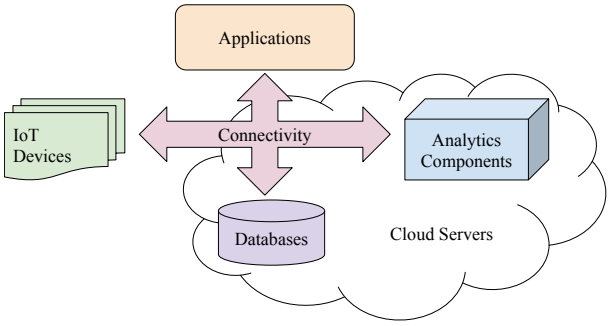

Fig. 1. General architecture of an IoT system

3) **Web application**: A software interface that allows for the remote access, control, and configuration of the IoT system.
4) **Connectivity**: The connectivity technology that allows for the communication between IoT devices, cloud servers, and the application.

A general architecture for an IoT system, constituted by the above building blocks, is shown graphically in Figure 1. As this architecture is already used in both IoT education [2], [1] and research [3], we use it to reason about our application-driven approach.

III. Related Work

IoT education has attracted the attention of the research community, and several approaches on how to design and teach a course on IoT have been published. We shed the light in this section on some recent works in that direction.

The authors in [13] present a systems-centric approach to design two IoT courses. The first course is based on introducing pervasive computing in general, with emphasis on the intelligence of things. The second course focuses on the process of testing a software-intensive system. These courses, however, specifically target computer science students, put more emphasis on system testing in the course design, and ignore the connectivity technologies aspect of an IoT platform. In [14], the authors introduce an IoT course in which students are expected to develop an open-source IoT middleware for a high-tech facility. The middleware acquires data from sensors that are installed on manufacturing equipment, stores that data, and provides controlled access via an API. Through teamwork, students learn how to build an industrial IoT system. The course is project-based and evaluates students from academic, business, and industrial perspectives. The authors of [15] develop a 12-hour course in which students are taught Arduino Vis(z)ual (ArViz) graphical programming language to build an IoT system. The course is oriented to junior high school students and aims to simplifying the programming aspect of IoT platforms. Another IoT course oriented to 6^{th} to 12^{th} graders is presented in [16]. The authors present a course design and implementation based on both software and hardware. The course is tailored to the skills of school students and aims to prepare them for engineering or computer science

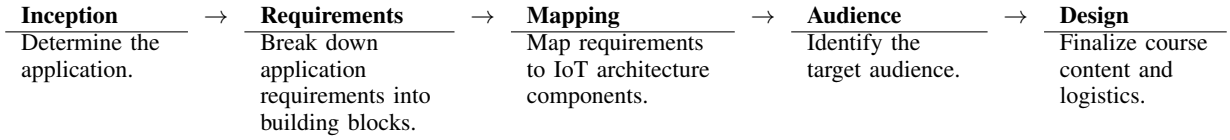

Fig. 2. Steps to plan an application-driven IoT course

programs at university. In [17], the authors design a massive open online course (MOOC) for IoT, and use smart home as a potential core project for the course. The students are tasked with building an IoT-based smart home and go through all the required IoT concepts to realize this project. Both theoretical and practical angles of IoT are interspersed to enrich the students' experience. A project-based IoT course is presented in [13], where students are involved in both practical projects and research-oriented projects. In [18], the authors point out that validation of IoT products is missing from university IoT courses and the use of inexpensive hardware – which are not used in consumer products – is dominant in these courses. Therefore, the authors suggest that IoT courses should use devices of a quality similar to that of end-consumer products. The author in [19] focuses on IoT-based smart homes and highlights the importance of security and privacy in smart home environments. The author notices that IoT education has a major gap in terms of covering security and privacy concepts. As such, a set of comprehensive hands-on lab tasks related to smart home security is proposed. In [20], the authors present a project-based IoT course in which building systems for a smart campus is targeted. In the course project students are tasked with building IoT platforms that can solve problems pertinent to campus operations.

Most of the reviewed literature finds value in project-based learning for IoT education. Also, involving the industry and subject matter experts from various sectors is becoming a trend [13], [14], [18]. These observations, along with the points highlighted earlier in Section I, inspire us to introduce our *application-driven IoT education* concept in the next section.

IV. Application-Driven IoT Education

With all the observations that have been highlighted earlier on the state of the art IoT education, we introduce the new approach of *application-driven* IoT education. Our aim is to build a complete course that revolves around a specific application that is of interest to a targeted group of learners. Example applications include connected cars, health and fitness monitoring, intelligent irrigation, fire detection, home automation, air pollution monitoring, smart grids, and so on. Planning for an application-oriented IoT course goes over the following steps (illustrated in Figure 2):

1) **Inception**: Decide on the application of interest.
2) **Requirements**: Determine the application requirements and organize them into building blocks.
3) **Mapping**: Map the requirements' building blocks to the constituent components of the IoT architecture.
4) **Audience**: Specify for whom this course is designed, and fix prerequisite background.
5) **Design**: Create the course material, logistics, and supplies.

We now elaborate more on these steps. On **inception**, the educator identifies, from the wide space of IoT-based applications, the application that they are interested in teaching. By studying this application deeply, the educator should build a clear case on the **requirements** to realize this application. These requirements must be broken down into well-defined building blocks. That is, the educator should describe what the application requires in terms of:

- **Data**: Specify the amount of data, type of data, and frequency of data collection for the respective application.
- **Analysis**: Determine the complexity and type of data analysis, as well as whether it can be conducted on the IoT device platform or requires a more resourceful server.
- **Actions**: Discuss what actions are possible based on the outcome of the data analysis.
- **Communication**: Describe the communication and networking technologies that best suit the application.
- **User interface**: Provide the specifications of the user interface that interacts with data collection and data analysis modules.

The ability of the educator to prepare this type of granularity when presenting the application to the learners will facilitate the **mapping** of the application requirements to the IoT architecture components as shown in Figure 3. In this figure, we show that deciding on the *data* and its collection along with the *actions* to be taken will help in specifying what IoT devices are needed. In particular, the sensor platform and actuator comprising the IoT device can be fully identified once a complete description of the information of interest to the selected application is provided. Furthermore, the scale and complexity of the application will dictate how intensive the data *analysis* is. Depending on this analysis, there will be a decision to be made on whether to do the analysis locally on the IoT device platform (lightweight analysis) or remotely at the cloud server side (heavyweight analysis). The *user interface* specifies what information the application users would like to view, and what configuration and management options they may have through a user-friendly web application interface (*e.g.*, to be run on handheld devices). Finally, by describing the *communication* infrastructure needed to realize the application, a decision can be made on what connectivity technologies best fit the application.

By completing the mapping step, the IoT course plan has taken its shape and the educator is ready to decide on the

Component		Requirement Type
IoT devices	⇒	Data; Analysis; Actions
Cloud servers	⇒	Analysis
Web application	⇒	User interface
Connectivity	⇒	Communication

Fig. 3. Relationship between IoT architecture components and the application requirements.

audience and the course design. The **audience** refers to the targeted group of learners that have a common interest in the selected application. Deciding on the audience is essential to identify what knowledge (that is, course prerequisites) are required for the learners to qualify for taking the course. Finally, the **design** step refers to deciding on the teaching material (textbooks, references, handouts, and slides), grading policy and assessment schemes (the distribution of grades over assignments, quizzes, lab tasks, and a project), and logistics and supplies (teaching assistants and lab software and hardware).

It is to be noted that the teaching material must provide a comprehensive background about the application of interest so that the audience appreciates the need for an IoT platform to implement it. As such, the educator is expected to cover the application from various perspectives: historical background, what area the application tackles, challenges and opportunities, available supportive technologies, sectors that need it, application requirements, methods of implementation. This is essential to motivate the choices around the implementation of the IoT platform.

After making the case for using IoT, the time comes for educating the audience about IoT technologies, principles, and concepts to prepare the learners for working on their course project. The grading and assessment in this course should put more emphasis on hands-on tasks and projects as suggested in [8]. A suggested schedule for the application-driven IoT course, based on a 15-week semester, along with the assessment scheme is shown in Table I. Sample course assessments are provided in the Appendix.

V. Example Course: Security and Privacy in Smart Homes

In this section, we give a detailed example on how to apply our new course planning technique to design an IoT course with smart home security and privacy as the application.

A. Inception

Smart homes comprise of several IoT devices, and their pervasive nature generates a large quantity of personal data about users. Thus, security and privacy is critical to smart home IoT deployments. Through this course, we aim to give students an understanding of the scale of problems that can arise, and the techniques required to fix them.

B. Requirements

The requirements of this type of course are as follows:

- **Data**: When attempting to add security properties to a system, we consider all data generated or processed by the system to be in scope. As such, we do not limit the data to be secured to that of a specific device or cloud service; rather, we consider the entire smart home as a data source. This could be a massive deluge of data: processing data locally stored on individual devices, data stored in all online services that interact with these devices, and all of the data in transit between them.
- **Analysis**: Smart home device content could contain intimate knowledge of what its inhabitants are doing at any point of the day. For example, data from a smart alarm clock may request a smart coffee machine to brew a cup, which leads us to assume the user is now awake. On the other hand, if a motion-sensing camera is not transmitting video data, it likely means that the user is away or sleeping. In addition to data, metadata is also ripe for analysis. Metadata is especially useful when the underlying content is encrypted, as destination, source, and data length can still imply much about *why* a communication is happening; for example, just knowing that the alarm clock is sending a message to the coffee machine may be enough. This type of analysis can be done locally on device, but more involved analyses require a cloud server.
- **Actions**: The data analysis can be used honestly and maliciously. For example, a defender could use the data flow information between devices to set up anomaly detection [21], but an attacker could use this same data flow to correlate insights about the user and track them throughout their day, with potential for stalking or other forms of abuse [22].
- **Communication**: Smart home IoT devices speak over a cacophony of protocols using protocols like ZigBee, Z-Wave, Bluetooth, and Wi-Fi, with varying degrees of connectivity and security [23]. This communication is likely encrypted, but unencrypted traffic can be extracted over-the-air relatively easily (*e.g.*, [24]), and encrypted traffic still can be analyzed for its metadata, as discussed above.
- **User interface**: The most secure user interfaces are those that abstract most of the complexities away. User interfaces can be subverted, however, creating potential privilege escalation issues.

C. Mapping

We propose a unifying lab environment that maps these requirements to the IoT architecture. It would consist of the following components:

- **IoT devices**: These would be Raspberry Pi SBCs with attached sensors (*e.g.*, a DHT-11 temperature sensor) and actuators (*e.g.*, a buzzer), to simulate smart devices. These devices would communicate with the cloud server, sending sensor data and receiving actuator commands. These devices would primarily be used to study embedded systems security labs.
- **Cloud server**: This would ingest data as it arrives from the IoT devices, placing information into a SQL database.

TABLE I
SUGGESTED COURSE SCHEDULE AND WEIGHTED COURSEWORK FOR AN APPLICATION-DRIVEN IOT COURSE OVER A 15-WEEK SEMESTER.

Weeks	**Topic area**	**Coursework**
Weeks 1–5	Foundational lectures on application of interest	Weekly quizzes (5% each)
Weeks 6–10	Hands-on introduction to IoT concepts	Weekly labs (5% each)
Weeks 11–13	Group project work and complementary lectures	Group project (40%)
Weeks 14–15	Project presentations and demonstrations	In-class presentation (10%)

In implementation, the "cloud" could simply be a server on a different network segment, but could involve Amazon AWS or Google Cloud if pedagogically necessary. The cloud service would be used to study cloud systems security labs, as well as data privacy labs.

- **Web application**: The web application would be an interface to the database and analysis of the cloud server. It would display any smart home information and allow users to input new commands for the smart home's devices. It would be used to study web security labs.
- **Connectivity**: Primary connectivity is provided by the gateway router that links the IoT devices together and to the cloud server and the Internet. It could be built using OpenWrt, allowing for deployment flexibility. The router mediates the connection between the IoT devices and cloud services and could log or drop packets as they flow through the network. Having access to the gateway router would be used to study network security labs.

D. Audience

We plan on our course being broad enough to capture the interest of those who wish to study smart homes, security and privacy, or both. Students should be able to navigate our lab environment and perform guided investigations; as such, we assume they have basic systems and networking knowledge as a prerequisite. This type of course is suitable for upper-level undergraduate students, as well as introductory graduate students. The level of difficulty can be tuned by increasing or decreasing the complexity of the simulated smart home.

E. Design

Our proposed design utilizes our mapped requirements to provide an appropriate level of rigor for the course.

1) Labs: As this is a lab-driven course, we first discuss the content of the labs. Individual labs would translate fundamental security and privacy attacks to the smart home setting, *e.g.*, the classic buffer overflow attack [25] in a device, or cross-site scripting [26] on the web interface. Many security concepts are unique to smart homes, however; the limited resources for security on IoT devices, combined with the wealth of personal information on them, makes smart homes a valuable target. Thus, these labs should focus on these aspects. Students could investigate how an attacker can leverage the physical environment – sensors and actuators – for malicious ends. These labs could also investigate privacy aspects, attempting to draw conclusions from the available data on-device, on-cloud, or in-cloud.

The interconnected architecture of the labs would allow students to investigate exploit chaining, using one attack to trigger a different one. For example, a buffer overflow attack on a smart speaker could be used to send a malicious packet to a smart smoke detector and trigger its alarm. Students would also gain the skills to use this attacker mindset to build defenses in the smart home setting.

2) Course logistics: We now briefly discuss administrative items regarding a course of this nature. Ideally, the lab environment would be a part of the very classroom in which students learn. Students would thus immediately see how they were actively generating the data under analysis. Regardless, students should be given remote shell access to each of these devices, the router that connects them, and the cloud services that back the whole platform. This would enable distance learning if required. Teaching assistants would be necessary to help facilitate labs and troubleshoot issues with students. As for evaluation, we presume that the vast majority of the grading weight will be oriented around these labs, with a mix of formative practice assignments and summative lab reports and code demonstrations.

VI. CONCLUSION

In this paper, we have introduced the application-driven approach of teaching IoT. In this approach, the educator plans the IoT course by firstly deciding on the application of interest to him/her and then studies how the requirements of that application can be achieved by the IoT architecture. Contrary to the current approaches of teaching IoT that either rely on the traditional lecture-based learning or project-based learning, application-driven IoT learning uses the *application* as the main axis of the course and then educates the learners on how IoT platforms can be used to build and realize that application. This approach makes the course more appealing to learners that have the same interest in the same field (while possibly coming from diverse specializations). It even helps the educator better identify the qualifications and logistics necessary to accommodate all potential learners. Finally, the paper presents an example on how to apply the application-driven approach of teaching IoT using the application of security and privacy in smart homes.

As a future direction, it will be interesting to supplement this study with the feedback of the learners who tried one or more forms of IoT education. Also, collecting and reporting data about the performance of the learners and the quality of their projects based on different IoT learning approaches will provide more insights on the best way to approach IoT education.

ACKNOWLEDGEMENTS

This paper results from the Dartmouth College and American University of Kuwait (Dartmouth-AUK) fellowship program, as well as the SPLICE research program supported by a collaborative award from the National Science Foundation (NSF) SaTC Frontiers program under award number 1955172. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the sponsors. Any mention of specific companies or products does not imply any endorsement by the authors, by their employers, or by the sponsors.

REFERENCES

[1] M. Khanafer and M. El-Abd, "Stimulating research projects through teaching a course on the internet of things," in *2020 IEEE Global Engineering Education Conference (EDUCON)*, 2020, pp. 1758–1763.

[2] A. Bahga and V. Madisetti, *Internet of Things: A Hands-On Approach*. Hyderabad: Universities Press, 2015.

[3] P. Ray, "A survey on internet of things architectures," *Journal of King Saud University - Computer and Information Sciences*, vol. 30, no. 3, pp. 291–319, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1319157816300799

[4] P. M. Chanal and M. S. Kakkasageri, "Security and privacy in iot: A survey," *Wireless Personal Communications*, vol. 115, no. 2, pp. 1667–1693, 2020.

[5] K. Ronoh, E. Muli, E. Ngwawe, and S. Njuki, "Internet of things learning methodologies, teaching tools and teaching platforms," in *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, 2021, pp. 1–6.

[6] D. D. Ramlowat and B. K. Pattanayak, "Exploring the internet of things (iot) in education: A review," in *Information Systems Design and Intelligent Applications*, S. C. Satapathy, V. Bhateja, R. Somanah, X.-S. Yang, and R. Senkerik, Eds. Singapore: Springer Singapore, 2019, pp. 245–255.

[7] G. R. Kanagachidambaresan, *Introduction to Internet of Things and SBCs*. Cham: Springer International Publishing, 2021, pp. 1–18. [Online]. Available: https://doi.org/10.1007/978-3-030-72957-8_1

[8] M. Khanafer and M. El-Abd, "Guidelines for teaching an introductory course on the internet of things," in *2019 IEEE Global Engineering Education Conference (EDUCON)*, 2019, pp. 1488–1492.

[9] S. Rowland and R. Sundaram, "Incorporation of the internet of things within the introductory course on microcontrollers," in *2021 IEEE Frontiers in Education Conference (FIE)*, 2021, pp. 1–4.

[10] B. Burd, L. Barker, M. Divitini, F. A. F. Perez, I. Russell, B. Siever, and L. Tudor, "Courses, content, and tools for internet of things in computer science education," in *Proceedings of the 2017 ITiCSE Conference on Working Group Reports*, ser. ITiCSE-WGR '17. New York, NY, USA: Association for Computing Machinery, 2018, p. 125–139. [Online]. Available: https://doi.org/10.1145/3174781.3174788

[11] T. M. Jois, C. Moncaliano, K. Henderson, and A. D. Rubin, "WDPKR: Wireless device profiling kit and reconnaissance," in *Hot Topics in the Science of Security (HotSoS) Symposium*, 2021.

[12] O. Vermesan, P. Friess, P. Guillemin, H. Sundmaeker, M. Eisenhauer, K. Moessner, M. Arndt, M. Spirito, P. Medagliani, R. Giaffreda, S. Gusmeroli, L. Ladid, M. Serrano, M. Hauswirth, and G. Baldini, *Internet of Things – From Research and Innovation to Market Deployment*. Gistrup: River Publishers, 2014.

[13] N. Silvis-Cividjian, "Teaching internet of things (iot) literacy: A systems engineering approach," in *2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering Education and Training (ICSE-SEET)*, 2019, pp. 50–61.

[14] V. Podolskiy, Y. Ramirez, A. Yenel, S. Mohyuddin, H. Uyumaz, A. N. Uysal, M. Assali, S. Drugalev, M. Gerndt, M. Friessnig, and A. Myasnichenko, "Practical education in iot through collaborative work on open-source projects with industry and entrepreneurial organizations," in *2018 IEEE Frontiers in Education Conference (FIE)*, 2018, pp. 1–9.

[15] K. Chochiang, K. Chaowanawatee, K. Silanon, and T. Kliangsuwan, "Arviz: An iot teaching tool for high school students," in *2019 23rd International Computer Science and Engineering Conference (ICSEC)*, 2019, pp. 87–91.

[16] A. Jaklič, "Iot as an introduction to computer science and engineering: A case for nodemcu in stem-c education," in *2020 IEEE Global Engineering Education Conference (EDUCON)*, 2020, pp. 91–95.

[17] Z. Shi, J. Chen, and S. He, "Diy smart house : Exploration and practice of iot mooc education," in *2020 15th International Conference on Computer Science & Education (ICCSE)*, 2020, pp. 557–560.

[18] L. G. Seng, K. L. K. Wei, and S. J. Narciso, "Effective industry ready iot applied courseware - teaching iot design and validation," in *2020 IEEE Global Engineering Education Conference (EDUCON)*, 2020, pp. 1579–1583.

[19] Z. Trabelsi, "Iot based smart home security education using a hands-on approach," in *2021 IEEE Global Engineering Education Conference (EDUCON)*, 2021, pp. 294–301.

[20] E. Yamao and N. L. Lescano, "Smart campus as a learning platform for industry 4.0 and iot ready students in higher education," in *2020 IEEE International Symposium on Accreditation of Engineering and Computing Education (ICACIT)*, 2020, pp. 1–4.

[21] W. Zhang, Y. Meng, Y. Liu, X. Zhang, Y. Zhang, and H. Zhu, "Homonit: Monitoring smart home apps from encrypted traffic," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 1074–1088.

[22] I. Lopez-Neira, T. Patel, S. Parkin, G. Danezis, and L. Tanczer, "'internet of things': How abuse is getting smarter," 2019.

[23] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "Sok: Security evaluation of home-based iot deployments," in *2019 IEEE symposium on security and privacy (sp)*. IEEE, 2019, pp. 1362–1380.

[24] W. Albazrqaoe, J. Huang, and G. Xing, "Practical bluetooth traffic sniffing: Systems and privacy implications," in *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*, 2016, pp. 333–345.

[25] A. One, "Smashing the stack for fun and profit," *Phrack magazine*, vol. 7, no. 49, pp. 14–16, 1996.

[26] K. S *et al.*, "Cross Site Scripting (XSS)," https://owasp.org/www-community/attacks/xss/.

APPENDIX
SAMPLE COURSE ASSESSMENTS

The following are samples of an in-class quiz and a course project used in an application-driven IoT course.

A. Sample Quiz

Program a Raspberry Pi (RPi) board using Python to implement the following functionality:

1) Print the following opening menu to the user:
   a) Make the LED blink
   b) Control the LED by the LDR sensor
   c) Send an email with the state of the LED
2) If Option (a) is selected, then at a push of a button an LED makes five blinks and then the opening menu is printed to the user again.
3) If Option (b) is selected, then the LED becomes controlled by the LDR sensor for 15 seconds. After that, the opening menu is printed to the user again.
4) If Option (c) is selected, then at a push of a button an email is sent to inform the recipient of the state of the LED (ON or OFF). The user should provide the email of interest once Option (c) is selected. After the email is sent, the opening menu is printed to the user again.

In writing your program, you should use a class (call it **`LEDClass`**) that handles both turning the LED ON or OFF

and keeping the state of the LED. Build the needed circuit on your breadboard and connect it to the RPi.

B. Sample Course Project

1) Project Objectives:
   a) Demonstrate the understanding of the IoT architecture and its associated technologies.
   b) Realize a complete IoT system.
2) Project Problem:
   a) Work in a team of three students to design and implement a complete IoT system that serves the application covered in the course. The IoT system is constituted by the following:
      i) **IoT Device:** Use Raspberry Pi as an IoT device to monitor and collect data (using sensors) about a certain phenomenon.
      ii) **Web Application:** Use a framework (*e.g.*, Django) to develop a Web application with which the IoT device is able to communicate using a Web service (based on REST or WebSocket APIs).
      iii) **Cloud Server:** Program a node (like the ESP8266 NodeMCU) to operate as a server that stores and/or analyzes your data. You can also use any available cloud servers (like ThingSpeak) to handle the storage and/or analysis of the data.
   b) All project programming must be done using Python.
3) Project Deliverables:
   a) **Report:** Write a technical report that fully describes the system model of your project.
   b) **Presentation:** Use slides to present your project to the class within no more than 15 minutes.
   c) **Demo:** Demonstrate the project functionality to the class within no more than 15 minutes.