

Rethinking IoT Education: Is the Concept Truly Grasped?

Tomáš Kormaník ✉ 

Department of Computers and Informatics, FEI TU of Košice, Slovakia

Jaroslav Porubán ✉ 

Department of Computers and Informatics, FEI TU of Košice, Slovakia

Abstract

This paper focuses on the topic of the Internet of Things (abbr. IoT) in the context of higher education and academic understanding of it. When briefly looking at the IoT course curriculum at our department, we suspected that the curriculum contents are not adhering to the definition of IoT. The goal of our work was to pinpoint the correct definition of IoT, which can be used to bring contents of the IoT courses as close to the truth as possible. Secondly, we reviewed available articles and reviews of formerly and currently taught IoT or related courses and evaluated whether their approach and contents were correct when considering the definition of IoT. We summarise the issues present in existing works and identify which specific parts are problematic, according to our assessment. Improving IoT courses is crucial since it shapes a student's understanding of the IoT paradigm and allows them to use it or even develop it in the future. Provisioning our students with a needed set of skills will make them more suitable for research, development, and industry-related futures.

2012 ACM Subject Classification Applied computing → Interactive learning environments; Human-centered computing → Ubiquitous computing; General and reference → Surveys and overviews; Computer systems organization → Sensor networks

Keywords and phrases Internet of Things, Informatics Education, Higher Education, Computer Science Education

Digital Object Identifier 10.4230/OASICS.ICPEC.2025.11

Funding This work was supported by the Slovak Research and Development Agency under the Contract no. APVV-23-0408.

1 Introduction

The term IoT has quickly become popular among the scientific and industrial community. A multitude of products are made in accordance with this paradigm. In industry, various implementations of sensors and devices are being deployed in order to gather data and optimise processes. Educational institutions have to adapt to these changes, encourage their implementation in the educational process, and utilise them to their advantage if possible. Naturally, our primary focus will be on higher education of IoT, but we can apply many of the presented ideas or approaches to secondary or even elementary education. The most commonly observed approach in educational environments in general is to teach the topic with practical experience to tie theoretical knowledge to the real world. In our case, it means teaching IoT with IoT technologies. While this approach creates highly technical courses, the resulting methodologies and findings can be utilised in other fields of education to some extent.

When observing trends in scientific journals and search engines, we can see that the popularity of IoT topics is on the rise each year. While not being one of the hottest topics, its popularity is rising thanks to the improvements in hardware performance of devices, availability of low-priced *Single Board Computers* (abbr. SBC) and technological



© Tomáš Kormaník and Jaroslav Porubán;
licensed under Creative Commons License CC-BY 4.0

6th International Computer Programming Education Conference (ICPEC 2025).

Editors: Ricardo Queirós, Mário Pinto, Filipe Portela, and Alberto Simões; Article No. 11; pp. 11:1–11:8

OpenAccess Series in Informatics



OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

11:2 Rethinking IoT Education: Is the Concept Truly Grasped?

advancements, which open new possibilities for its use. The largest impact in recent years is undoubtedly caused by the increased availability and versatility of large language models, which can be utilised on the edge by devices themselves or by calling an API with the request. Along with a radical increase in network speeds, both wired and wireless, the number of IoT devices and data they transfer has naturally skyrocketed. Even fog computing architecture, which is supposed to move services closer to end devices, creates benefits for IoT implementations since it allows for architecture less dependent on the cloud itself.

2 Definition of IoT

The paradigm of IoT originated in 1982 with the creation of an early network-connected smart device in the form of a vending machine at Carnegie Mellon University [14]. Later, the term *ubiquitous computing* emerged, which presented hardware and software technologies seamlessly integrated into the environment, making them ambient and natural to interact with. The first mention of *Internet of Things* is publicly credited to Kevin Ashton during his presentation at *Procter & Gamble* [3]. He presented this paradigm, where computers can communicate freely and gather their information without human input or interaction.

A significant amount of time has passed, and multiple expanded definitions regarding IoT have been presented. Moreira et al. [12] note that there is no broadly accepted conceptual definition of IoT. Their understanding indicates that this term refers to physical objects that incorporate electronics which allow them to collect and share data. This understanding is fundamentally correct, but we consider it too broad since the ability to collect and share data across varied types of media is a general goal of any sensor.

A study by Ray et al. [18] talks about how pervasive, ubiquitous, and omnipresent nature is a key part of the definition for IoT. They consider this paradigm a widely spanning ecosystem, which is constantly growing thanks to the increasing number of devices connected to the internet. They point out that there will be more things connected to the internet than people in the future. While their understanding is accurate, they appear to underestimate the potential of IoT by describing it as an assistive solution.

The survey by Atzori et al. [4] agrees with the multiple definitions of IoT, but they attribute that to the fact that this paradigm is being considered from different points of view, providing slightly different understandings from each vision perspective. They present 3 different visions: things, internet, and semantic-orientated ones. After reviewing all the visions, we came to the conclusion that each has a significant amount of accuracy. From our perspective, the division of these focuses is primarily advantageous for research purposes, as it allows for the assignment of specific tasks to experts in each field, thereby facilitating more effective research and development.

Work by Perera et al. [15] is highly regarded and well accepted. It has already drawn attention to the importance of IoT in the year 2013. They consider big data one of the main reasons for the IoT's rise in popularity since this massive amount of data can be processed to provide information that was not available before. They are quoting multiple definitions, but the one they deemed most accurate is provided by Strategic Research Roadmap [21], which is: "The Internet of Things allows people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service." [21]. This definition seems to stem from the original definition by Kevin Ashton and expand it to a broader scope. When comparing this definition with others, its simplistic nature might seem off-putting, but the supporting article, which further explains it, provides relevant and sufficient reasoning for its broadness.

There are various other opinions and models of IoT presented. When relating to software engineering, these definitions and understandings of IoT usually look from the technical point of view. Commonly used are models which split infrastructure into **perception**, **network**, **middleware**, **cloud**, and **application** layers. Naturally, some examples and definitions merge or omit some layers, but overall understanding is, in the majority, the same. An overview of this topic is provided by Radouan Ait Mouha [1], which explains two main models and additionally a variety of sensors used in IoT.

3 Current state and challenges of IoT

We consider the most significant challenges to this paradigm to be the topics of **security** and **privacy**. Our core assumption is that an increased introduction of IoT devices to our daily lives, which we can already see is vast, will not only increase the number of potential targets but also the number of vulnerabilities in their source code. Ideal IoT devices will be communicating with large amounts of other devices, processing data gained from this communication, and again processing it with inputs from their own sensors and adapting to the environment seamlessly. This naturally creates more lines of code, and tied to that are an increased number of errors in the source code as well.

All of this creates new vectors of attacks, which can turn features of IoT networks into critical flaws. Droppa and Harkal [7] mention the growth of IoT devices as the first factor that will affect the cybersecurity landscape in the near future. They additionally mention current trends and predictions based on cited surveys and research, which all indicate growth in threats that can use or target IoT devices as well, therefore doubly increasing the importance of the aforementioned topics of **security** and **privacy**.

In a survey by Noor and Hassan [5] published in 2016, they identified authentication as the most popular technique on which researchers focused in this field. We can also observe that encryption was not that popular, which makes sense when we consider the fact that most IoT devices have a low amount of computing power at their disposal. They also present a familiar 3-layer model of the IoT security landscape, which is widely used in academia and industry. Schiller et al. [19] have looked at the landscape of security in 2022, where they still stated the same problems as presented by Noor and Hassan. The evidence indicates security concerns and known issues have not diminished, but on the contrary, they are slowly rising. Even when looking at recent contributions, Hassain et al. [9] have pointed out similar issues; however, they highlight that privacy concerns are currently most prevalent. This is understandable and relates to the increase in available IoT devices, which allows a larger number of people to observe the impact and potential of this technology. Recent contributions use artificial intelligence and machine learning to address these issues. Notable are works by Kalakoti et al. [10], who are attempting to detect botnets; Karthikeyan et al. [11], who are creating intrusion detection solutions; and, at last, Aldhaheeri et al. [2], who are analysing this landscape from their perspective and providing useful statistics and summaries.

Current IoT devices and networks are trading the openness sought by IoT devices for security and privacy. Most solutions rely on centralised management, where data and communications from all IoT devices go through one or multiple servers. Such an arrangement goes against the decentralised and open definition of IoT but serves as a necessary tradeoff since these servers allow for control and enable both aforementioned security and privacy. A fitting example in this case is Apple's so-called *Find My Network*, which allows their users to find any of their devices bound to their *AppleID* anywhere in the world. Dependence on the *AppleID* allows Apple to maintain control over the *Find My Network*. When we look at

11:4 Rethinking IoT Education: Is the Concept Truly Grasped?

a device like AirTag, it fits the IoT definition for the Thing since by only connecting it to the internet through Apple devices, its usability is vastly expanded. Normally, this device would have highly limited usability because it only has Bluetooth Low Energy; however, by turning essentially all iPhones into a global mesh of Bluetooth hotspots, the AirTag became a significant component of the Internet of Things.

4 Present education of IoT & with IoT

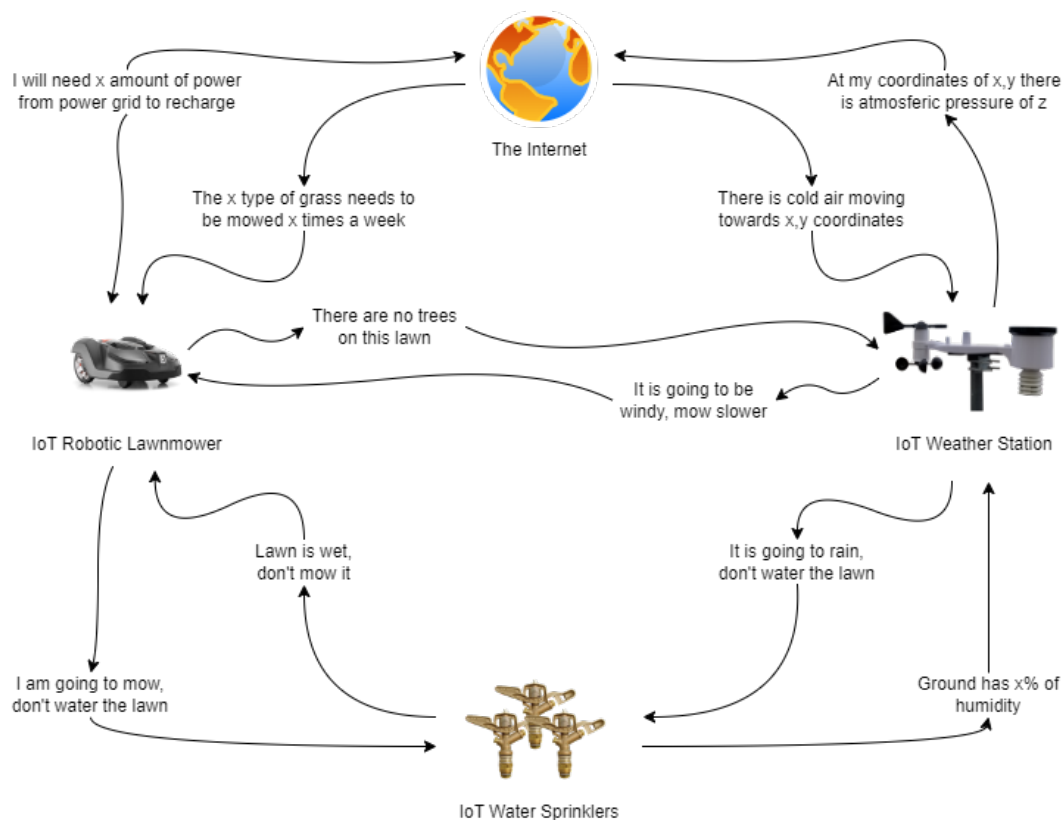
It is crucial to determine if specific education curricula consider IoT as a paradigm that students are taught about and for or if they simply consider it as a medium to teach students different knowledge. The IoT paradigm can be used to teach any subject with different success rates depending on facilities, course design, and groups of students. We have analysed the landscape from both objective and subjective perspectives.

Courses at our university are endorsing both approaches, therefore teaching IoT with IoT. Courses utilise devices of the *Raspberry Pi* family, along with a multitude of sensors, smart devices, and software. Students are supposed to utilise their previously gained knowledge in software engineering to successfully connect peripherals to *Raspberry Pi* directly or through a network and design software to utilise information gained from these sources to enrich or improve space around them. Examples of resulting projects created during the IoT course can be some sort of integrated smart home appliances, software middleware facilitating management of smart devices, and similar. We already hinted that results of this course are not entirely aligned with the IoT paradigm, and we think the contents of this course can be improved in order to make students understand IoT more clearly. However, when we objectively evaluate the curriculum at our institution, we consider it one of the best since it teaches students skills necessary to potentially work with IoT devices.

Gomez et al. [8] have utilised the technology of digital twins in their research to teach students about components of computers. Based on their publication, we consider their programme farther from the actual IoT course, even though the definition of IoT they state in their article is the 2nd most accurate one, which proves uncertainty about IoT understanding. The evidence demonstrates that they either do not fully understand the definition or, during the design phase of their course, they misinterpreted the meaning of available knowledge.

Significantly better is the research performed by Dobrilović et al. [6], which utilises the open-source platform *Arduino* and its many plug-in modules. They base their education on the 5-layer model of IoT, which is just a more granular specification of the aforementioned broad definition. It mentions middleware as part of this paradigm, which is not always correct but is the most commonly accepted model of IoT architecture among the publicly available education curricula in the Slovak Republic and Czech Republic (we have ongoing research evaluating IoT university courses worldwide, but only these results are currently verified). We have come to the conclusion that this model is useful because a variety of solutions can be designed and implemented with it in mind in professional and educational settings, boosting understanding and clarity of the topic. Relating models: some researchers mention or utilise 4- or even 3-layer models proposed by other researchers. These models can be viewed as technicalities because they essentially share the same fundamental concept. Regarding actual implementation, of course, working with these sensors, modules, and devices can definitely bring students closer to understanding and being able to work with IoT technologies in the future.

There are numerous works available that analyse the overall state of education in relation to IoT. One of the best is work by Natalia Silvis-Cividjian [20], which correctly understands the complexity of the IoT paradigm and suggests a complex and well-designed course that teaches



■ **Figure 1** Example diagram of communication in a garden enhanced by IoT-enabled devices.

related knowledge to pervasive computing as well. There are still some misinterpretations and issues present, but they don't decrease the value of the resulting work. For us, work by Rajora et al. [17] is most relevant. They correctly identify key benefits of IoT in education; they predict that educational institutions need to adapt to teaching with this paradigm in mind. Even when considering the paradigm's issues, they still recommend adding IoT to education. They provide a guide on how to effectively utilise IoT in education, which has some weak points but also points we can learn from.

5 Possibilities for improvement

The current state of technology is evident. Some institutions have minor differences in their IoT-related courses, but the majority are utilising SBCs along with a variety of sensors and peripherals to create devices programmable by students. For programming, usually languages such as “C” or “Python” are used, although some courses incorporate “C++” or “Java” to follow up on previous knowledge. All of these courses serve only demonstrative purposes (courses at our department as well), mainly showing students use cases for *Raspberry Pi* and other devices, rather than actually exposing students to IoT.

We suggest that more rigorous education in terms of theory and logical thinking is needed. While tinkering with SBCs is entertaining for students, it is important that the actual solutions they create adhere to the standards and needs of the IoT paradigm. Often we can't avoid using centralised online services in IoT solutions, but utilising open data, neighbouring

11:6 Rethinking IoT Education: Is the Concept Truly Grasped?

IoT devices, and local sensors should be preferred. The rapid growth of AI opens various new possibilities for IoT in terms of data analysis and acquisition. We expect that in the near future we will witness the arrival of a broad assortment of IoT devices with dedicated hardware for AI.

So far, we have draughted various improvements to our lectures and courses to present IoT not as a concept or playing with SBCs but as a paradigm. Our current goal is to deepen the understanding of students in terms of processes and technologies in this field. One of our prototype example models is the so-called “IoT Garden,” which helps us explain the IoT paradigm from basics to more complex concepts. The appended diagram (Fig. 1) shows a simplistic model of this solution, which demonstrates the benefits of communication between things themselves. This approach should lead to the understanding that the Internet of Things components share information between each other to benefit themselves or any other device on the Internet.

In our case, we can utilise already available resources and environment at our department, especially well-tested OpenLAB¹ laboratory, which is built as a platform equipped with IoT-enabled sensors and peripherals. This open and easily accessible platform for testing and deployment of solutions is ideal for project-based learning (abbr. PJBL). Mursid et al. [13] say that this way of teaching encourages students to think creatively and get along with others. We believe that this approach is directly advantageous for teaching the IoT paradigm since its main idea is abstract and needs creativity to be put into practice. PJBL allows for a more personal approach since, in general, it gives students enough freedom to use their creativity. Coincidentally, this type of curriculum can motivate some students to perform since they can express themselves.

6 Conclusion

The definitions of IoT are numerous, and none is specifically labelled as the correct one. This diversity stems from the fact that IoT encompasses hardware, software, and networking fields and their subfields. Each field mentions a different definition, which can cause confusion between each of them. Therefore, the finite definition of the whole IoT paradigm needs to be broad and open to align with all fields. We deemed the definition by Strategic Research Roadmap [21] as most relevant and proceeded in its use in our draft materials for the improved IoT course. When used in an educational setting, it became clear that such a broad definition was not sufficient and was more philosophical than practical. Due to this circumstance, we deemed the definition which leaned on the 5-layered model of IoT architecture as the best compromise for all use cases.

Recent IoT courses have generally featured similar curricula and scenarios. In the past decade, institutions have been inspired by each other, which has resulted in rather standard curricula, with only minor differences among courses. Due to technical and scientific advancements, major restructuring of these courses is relevant. We determined that these courses are focused on practical skills, whether they are conducted in electronics-related or software engineering study programs at universities. Since our focus is software engineering, we desire to steer our course towards a deeper theoretical understanding of the IoT paradigm and its concepts. Since IoT is utilised for green and distributed solutions, nurturing skills to create these solutions is relevant.

¹ For more detailed information about OpenLAB refer to work from the time of its creation [16]

In the future, we aim to create a complex review of available and documented IoT courses or curricula, highlighting issues and benefits of each. This will allow us to create a state-of-the-art IoT course, which will then be adapted to the aforementioned ideas and concepts.

References

- 1 Radouan Ait Mouha. Internet of things (iot). *Journal of Data Analysis and Information Processing*, 9(02):77, 2021. doi:10.4236/jdaip.2021.92006.
- 2 Alyazia Aldhaheri, Fatima Alwahedi, Mohamed Amine Ferrag, and Ammar Battah. Deep learning for cyber threat detection in iot networks: A review. *Internet of Things and Cyber-Physical Systems*, 4:110–128, 2024. doi:10.1016/j.iotcps.2023.09.003.
- 3 Kevin Ashton et al. That ‘internet of things’ thing, 2009. Accessed at 2025-01-10. URL: <https://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf>.
- 4 Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer Networks*, 54(15):2787–2805, 2010. doi:10.1016/j.comnet.2010.05.010.
- 5 Mardiana binti Mohamad Noor and Wan Haslina Hassan. Current research on internet of things (iot) security: A survey. *Computer Networks*, 148:283–294, 2019. doi:10.1016/j.comnet.2018.11.025.
- 6 Dalibor Dobrilić, Z Čović, Ž Stojanov, and Vladimir Brtko. Approach in teaching wireless sensor networks and iot enabling technologies in undergraduate university courses. In *Proceedings of the 2nd regional conference Mechatronics in Practice and Education, MechEdu*, pages 18–22, 2013. doi:10.13140/rg.2.1.4262.9608.
- 7 Martin Droppa and Marcel Harakal. Analysis of cybersecurity in the real environment. In *2021 Communication and Information Technologies (KIT)*, pages 1–7, 10 2021. doi:10.1109/KIT52904.2021.9583748.
- 8 Jorge Gómez, Juan F. Huete, Oscar Hoyos, Luis Perez, and Daniela Grigori. Interaction system based on internet of things as support for education. *Procedia Computer Science*, 21:132–139, 2013. The 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2013) and the 3rd International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH). doi:10.1016/j.procs.2013.09.019.
- 9 Mahmud Hossain, Golam Kayas, Ragib Hasan, Anthony Skjellum, Shahid Noor, and S. M. Riazul Islam. A holistic analysis of internet of things (iot) security: Principles, practices, and new perspectives. *Future Internet*, 16(2), 2024. doi:10.3390/fi16020040.
- 10 Rajesh Kalakoti, Hayretin Bahsi, and Sven Nömm. Improving iot security with explainable ai: Quantitative evaluation of explainability for iot botnet detection. *IEEE Internet of Things Journal*, 11(10):18237–18254, 2024. doi:10.1109/jiot.2024.3360626.
- 11 M Karthikeyan, D Manimegalai, and Karthikeyan RajaGopal. Firefly algorithm based wsn-iot security enhancement with machine learning for intrusion detection. *Scientific Reports*, 14(1):231, 2024. doi:10.1038/s41598-023-50554-x.
- 12 Filipe T. Moreira, Andreia Magalhães, Fernando Ramos, and Mário Vairinhos. The power of the internet of things in education: An overview of current status and potential. In Óscar Mealha, Monica Divitini, and Matthias Rehm, editors, *Citizen, Territory and Technologies: Smart Learning Contexts and Practices*, pages 51–63, Cham, 2018. Springer International Publishing. doi:10.1007/978-3-319-61322-2_6.
- 13 R Mursid, Abdul Hasan Saragih, and Rudi Hartono. The effect of the blended project-based learning model and creative thinking ability on engineering students’ learning outcomes. *International Journal of Education in Mathematics, Science and Technology*, 10(1):218–235, 2022. doi:10.46328/ijemst.2244.
- 14 CMU School of Computer Science. Network connected coke machine history, 1982. Accessed at 2024-12-16. URL: <https://www.cs.cmu.edu/~coke/coke.history.txt>.

- 15 Charith Perera, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. Context aware computing for the internet of things: A survey. *IEEE Communications Surveys & Tutorials*, 16(1):414–454, 2014. doi:10.1109/surv.2013.042313.00197.
- 16 J. Porub  n. Challenging the education in the open laboratory. In *2018 16th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, pages 439–444, 2018. doi:10.1109/ICETA.2018.8572247.
- 17 Ricky Rajora, Aarju Rajora, Bhanu Sharma, Priyanshi Aggarwal, and Siddhant Thapliyal. The integration of iot in learning environments: Assessing the impact of educational empowerment and addressing its challenges. In *2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM)*, pages 1–5, 2024. doi:10.1109/iciptm59628.2024.10563682.
- 18 Sandip Ray, Yier Jin, and Arijit Raychowdhury. The changing computing paradigm with internet of things: A tutorial introduction. *IEEE Design & Test*, 33(2):76–96, 2016. doi:10.1109/mdat.2016.2526612.
- 19 Eryk Schiller, Andy Aidoo, Jara Fuhrer, Jonathan Stahl, Michael Zi  rjen, and Burkhard Stiller. Landscape of iot security. *Computer Science Review*, 44:100467, 2022. doi:10.1016/j.cosrev.2022.100467.
- 20 Natalia 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)*, volume 41, pages 50–61, 2019. doi:10.1109/icse-seet.2019.00014.
- 21 Ovidiu Vermesan, Peter Friess, Patrick Guillemin, Sergio Gusmeroli, Harald Sundmaeker, Alessandro Bassi, Ignacio Soler Jubert, Margaretha Mazura, Mark Harrison, Markus Eisenhauer, et al. Internet of things strategic research roadmap. In *Internet of things-global technological and societal trends from smart environments and spaces to green ICT*, pages 9–52. River Publishers, 2022. doi:10.1201/9781003338604-2.