International Journal of Electrical and Computer Engineering (IJECE)
Vol. 14, No. 6, December 2024, pp. 7236~7243
ISSN: 2088-8708, DOI: 10.11591/ijece.v14i6.pp7236-7243

Evolution of the concept of device moving from internet of things to artificial intelligence of things

Gaetanino Paolone[1], Francesco Pilotti[2], Andrea Piazza[1]
[1]B2B S.r.l., Teramo, Italy
[2]Gruppo SI S.c.a.r.l., Teramo, Italy

Article Info

Article history:

Received May 15, 2024
Revised Aug 1, 2024
Accepted Aug 6, 2024

Keywords:

Artificial intelligence of things
Computing paradigm
Edge
Fog
Internet of things
Internet of things architecture
Internet of things device

ABSTRACT

The internet of things (IoT) refers to a network of physical devices that are embedded with sensors, software, and network connectivity, allowing them to collect and share data. The devices are the core of any IoT ecosystem. Browsing the extant literature, it emerges that the meaning of the term device depends on the reference context. It follows that, it is an important topic to investigate the reasons behind such a degree of indeterminacy. This paper elaborates on the evolution of the concept of device moving from IoT to artificial intelligence of things (AIoT). The finding that comes from this study is that this evolution is a direct consequence of the evolution of the IoT computing paradigms.

Corresponding Author:

Gaetanino Paolone
B2B S.r.l.
Via Enrico Fermi 9, San Nicolò a Tordino, 64100 Teramo, Italy
Email: g.paolone@b2binformatica.it

1. INTRODUCTION

The internet of things (IoT) is a network of physical devices, interfaces, and other items embedded with sensors, actuators, electronics, and connectivity. Table 1 shows the number of IoT connected devices worldwide from 2019 to 2023, with forecasts until 2028 [1]. At a high level of abstraction, an IoT infrastructure includes the following basic components:

Table 1. Connected IoT devices in billions

Year	Connected devices	Year	Connected devices
2019	8.60	2024	17.08
2020	9.76	2025	19.08
2021	11.28	2026	21.09
2022	13.14	2027	23.14
2023	15.14	2028	25.21

- Sensors gather real-time data from the environment. Figure 1 shows a generic device with three embedded sensors (an alarm sensor, a temperature sensor, and a proximity sensor). Fridges, televisions, wearables, smartphones, and cars are everyday instantiations of the generic device in the figure.
- A sensor converts a physical phenomenon, such as a sudden rise of the temperature in a room, into a digital signal. That signal is then converted into a readable format that a human or machine can interpret and act on. The power consumption and precision of sensors affect the quality of service of the IoT

solution. Sensors can function in either digital or analog mode. There are two main types of sensors used in IoT systems: passive sensors (they detect changes in their environment without any dedicated power supply) and active sensors (they require some form of power source to function, *e.g.*, a battery). Self-powered sensors are an interesting category of devices since they can generate their own power, typically through kinetic energy or by using 5G, for example, as a power source [2].

- Microcontrollers process and manage the data collected by the sensors, often performing tasks like filtering and calibration. A microcontroller is an integrated circuit that commonly includes a processor, memory and input/output (I/O) peripherals. Microcontrollers are designed to govern specific operations. According to a report by precedence research [3], the global microcontroller market was valued at USD 27 billion in 2022 and is expected to reach USD 69 billion by 2032.
- Communication modules transmit data over the network. Examples of this component include satellite, Wi-Fi, or Bluetooth.
- Cloud supports IoT devices and applications. It includes the underlying infrastructure, servers and storage, needed for real-time operations and processing.
- User interface (when present) converts the information for consumption. It could be a live monitoring display or a notification when pre-set limits are reached.

Figure 1. A “generic” IoT device with embedded sensors

As IoT devices special generate large amounts of data from different sources and type of sensors, then artificial intelligence (AI) (and in special way machine learning (ML) a component of the more generic AI term) will be functionally necessary to deal with these huge volumes to make more sense of that data. Data is only useful if it creates an action. To make data truly actionable, it needs to be supplemented with context. Artificial intelligence and internet of things together (shortly, AIoT) are the context, *i.e.*, connected intelligence and not just connected devices [4], [5].

By browsing the largest curated databases (namely, ACM, IEEE, Scopus, Springer, and Elsevier) we found that this acronym was mentioned for the first time in [6], but the paper was submitted in 2016. AI is beneficial for both real-time and post event processing:

- Real-time processing allows responding quickly to specific situations in case of abnormal behavior. This approach is very useful, for example, in the remote monitoring of elderly citizens staying at home.
- Post event processing, on the other side, allows identifying patterns in data sets and running predictive analytics (*e.g.*, setting a correlation between traffic and parking usage, or setting a correlation between air pollution and chronic respiratory illnesses within a city center).

IoT, augmented and enhanced by ML, is multiplying the impact and benefit to firms that are adopting these complimentary technologies. In fact, AI can be an integral element for success in today’s IoT-based digital ecosystems. The reason is simple. Combining IoT with rapidly advancing AI technologies can create “smart machines” that simulate intelligent behavior to make well-informed decisions with little or no human intervention. As new technology applications emerge where IoT works hand in hand with AI – the resulting innovations are proving how IoT can create new markets and opportunities, create value, disrupt traditional business models and dramatically change the competitive landscape. The benefits deriving from the marriage of AI and IoT have been highlighted for all IoT application domains, such as: smart cities [7], [8]; healthcare [9], [10]; retail [11]; and industry [12].

This study investigates the meaning of the term “device” in the following four occurrences: (IoT) device, smart (IoT) device, (IoT) Edge device (occasionally, the Edge (IoT) device diction is used. See for example [13]), and (IoT) Edge computing device. The meaning is linked to the computing paradigms cloud, Edge-cloud, and Edge AI. The research aims at clarifying what is the correct meaning of the four terms listed above and where their denomination comes from. Therefore, it aspires giving a contribution to clarify when each of the above four phrases should be used and why. This work is the result of the reading of a large number of studies appeared in the IoT/AIoT literature. As sources, we retrieved papers published by ACM, Elsevier, IEEE, and Springer; in addition, the Scopus curated database was queried. The selected studies span the years from 2004 to 2024.

The paper is structured as follows. Section 2 recalls the cloud, Edge, and Edge AI computing paradigms; while section 3 compares the definition of smart device given in two recent articles [14], [15]. Both those papers have investigated the meaning of the concept of smart device, its main features, as well as its role in the IoT. In light of the content of section 2, 3 and 4 attributes the correct meaning to the four terms mentioned above. Then, section 5 discusses the limits of the present study, while section 6 ends it.

2. COMPUTING PARADIGMS

This section recalls the cloud, the Edge, and Edge AI computing paradigms. Such a primer is based on current literature. This excursus is necessary to point out their basic characteristics, a prerequisite necessary to understand the conceptual framework where the meaning of the four terms mentioned in the Introduction comes from

2.1. The cloud computing paradigm

In Gershenfeld *et al.* [16] described the scenario of one network (that they called internet-zero) connecting "things." In such a scenario, the things are all kinds of everyday devices that sense the environment and send what they have sensed to either a local or global computer (the modern cloud). Figure 2 shows the IoT architecture that corresponds to such a perspective.

The perception layer consists of sensors and actuators. Broadly speaking, the sensors are things that detect and respond to environmental changes, which may come from a variety of sources such as temperature, pressure, light, proximity, and motion. Most of the sensors available on the market need a battery, which poses the issue of the periodic battery replacement. An important line of research concerns the development of battery-free radio frequency identification (RFID) tags (called passive sensors in [17]) as an option in the deployment of future IoT systems.

The network/communication layer supports the connectivity among the devices being part of the IoT network. At this stage, a plenty of protocols may be involved (*e.g.*, hypertext transfer protocol (HTTP), message queuing telemetry transport (MQTT), and constrained application protocol (CoAP)). Kassab and Darabkh [18] and Sobin [19] provide a lot of details about the communication protocols that play a fundamental role in the orchestration of data transfer among the layers and the different participants in actual IoT systems.

The application layer is the front end of the architecture in Figure 2. This layer provides IoT developers with suitable software tools essential in the implementation of IoT applications in the well-known domains of smart health, smart cities, smart homes, intelligent transportation, and so on [20]. The application layer benefits of the resources featured by the cloud fundamental to process the big volumes of data that come from the network layer, according to the applications' requirements.

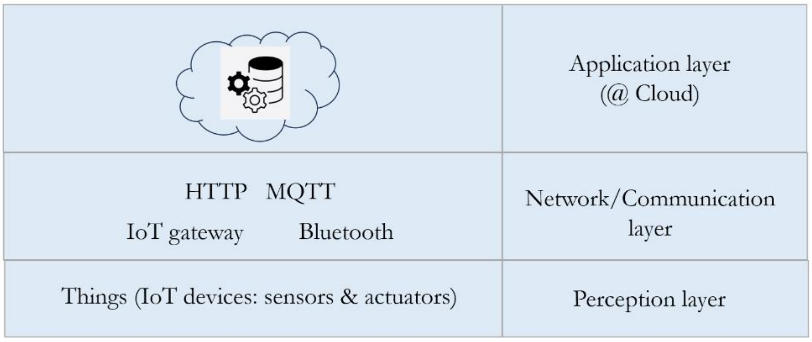

Figure 2. The cloud-oriented architecture of IoT systems

2.2. The Edge computing paradigm

For long time, the deployment model of IoT systems has been the cloud since it offers unlimited storage and computing power on-demand. Unfortunately, connecting IoT devices directly to the cloud poses issues concerning, among the many, security, privacy, network congestion, and, consequently, performance degradation. To mitigate these concerns, it has been stressed that the architecture of modern IoT systems should include, besides the things layer and the cloud layer, also an Edge layer and a Fog layer [21]–[25]. Given the purposes of the present study, in the following the Fog layer is ignored.

In the Edge-cloud (EC) architecture as shown in Figure 3, the Things layer consists of fixed-place devices (*e.g.*, smart fridges and smart surveillance cameras) and/or mobile devices (*e.g.*, smart wearable devices, smartphones, and vehicles) giving rise to specific applications (*e.g.*, smart building, traffic monitoring, and healthcare). These devices embed sensors and micro-controller units (MCUs), so they can carry out some degree of computation. The mode of communication between the things and the Edge devices is wireless in nature, while the Edge can communicate with the cloud using both wired and wireless means of communication. The Edge layer is supplied with dedicated routers and switches that act as gateways to the cloud. Moreover, it is equipped with micro-data centers able to collect the sensed data by the IoT devices, filter them, and off-load the filtered data to the cloud resulting in an enormous bandwidth saving.

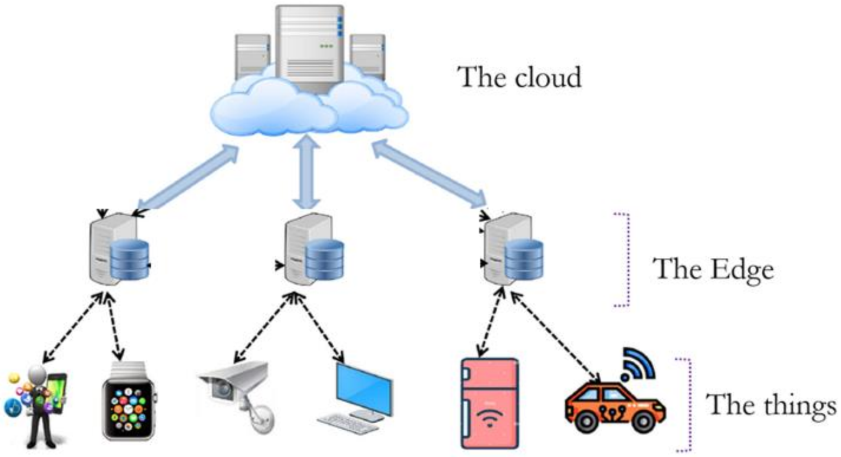

Figure 3. The EC architecture

2.3. The Edge AI computing paradigm

Running ML algorithms in the cloud is painless, while running them on edge-side electronic devices is critical due to the lack of sufficient computing resources. It has been pointed out that distributing the processing of ML algorithms between the Edge and the cloud is the solution that solves many of the problems mentioned in subsection 2.2 [26]. Market research future predicts that the global EC technology market could reach $170 billion between 2020 and 2030. This enormous growth in the market of hardware devices and related embedded software that can process ML algorithms is combined with the great impulse coming from the world of research where scholars are exploring how far the processing of big data can be pushed in proximity of the IoT devices that collected the data, *i.e.*, at the Edge side. The edge learning machine (ELM) is an open-source framework able to support developers in designing and deploying ML solutions on Edge devices [27]. ELM manages the training phase on a desktop computer and performs inferences on MCUs. Currently, the framework implements three well-known supervised ML algorithms. Microsoft is developing EdgeML (*https://www.microsoft.com/en-us/research/project/edgeml/*), a library of ML algorithms that are trained on the cloud and can run on resource-constrained edge IoT devices.

The term Edge AI (or AI at the Edge) summarizes the scenario we are talking about. In other words, the term Edge AI implies that the ML algorithms are run close to where the data is actually collected (usually by making usage of MCUs directly connected to the sensors immersed in the physical environment and which are part of the IoT system), or in a dedicated hardware (often called Edge server or micro-data center, see subsection 2.2) located near by the sensors. Sipola *et al.* [28] is a very detailed review work on Edge AI. It is divided into three parts concerning: the applications that can benefit from it; the hardware suitable for implementing Edge AI and finally the APIs that facilitate pursuing this objective.

The term Edge AI and the sentence "Edge AI computing paradigm" coincide, respectively, with the term Edge intelligence and the sentence "AI-based Edge-cloud architecture" in [29]. In light of recent studies (*e.g.*, in studies [30]–[32]), the architecture appropriate to implement the Edge AI paradigm is that shown in Figure 4. The brain icon in the figure denotes that intelligence is present in both sides, which makes possible a cooperative computation (*i.e.*, the processing takes place part in the IoT device and part in the Edge server).

Tiny machine learning (TinyML) is a field related to Edge AI. The TinyML community was born in 2019 with the aim of developing algorithms, software and hardware to make it possible to run ML models on electronic devices with limited resources and at low cost. In study [33], the Edge AI paradigm has been adopted to implement an Edge AI-based vehicle tracking solution as part of a smart parking system.

The emergence of TinyML has positively revolutionized the field of AI by promoting the joint design of resource-constrained IoT hardware devices and their learning-based software architectures. By adopting TinyML, IoT devices gain the ability to analyze data on their own, accelerating decision making, while dramatically simplifying IoT system architecture. In [34], [35] are two in-depth surveys on the topic. The deployment of pre-trained ML models on the cloud into edge devices is now possible, after performing some compression of those models and optimization of the inference stage [36]. The consequence is that, thanks to TinyML, it is becoming feasible the analysis and interpretation of data directly on the IoT devices and, when necessary, start reaction in real-time.

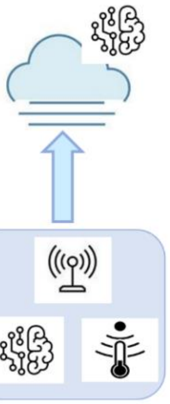

Figure 4. The architecture that supports Edge AI

3. THE NOTION OF SMART DEVICE

Silverio-Fernández *et al.* [14] carried out a survey in order to answer the following question: "What does mean smart device/thing?" The goal of the work was to converge to a unifying definition for such a notion, since at the moment the authors performed the study, the question was not answered. In light of the review outputs, Authors [14] defined a smart device in terms of three basic attributes: Contextawareness, Connectivity, and Autonomy. In turn, context-awareness means that smart devices are able to sense data from the environment through sensors; connectivity is a precondition so that they can exchange data (either wire or wirelessly) with other devices; autonomy denotes the capability of the electronic device to perform autonomous computing.

Rokonuzzaman *et al.* [15] carried out another survey in order to answer the same question at the origin of the survey carried out by Silverio-Fernández *et al.* [14] (incidentally, this work does not mention the previous one, likely because authors did not know about). In light of the review outputs, Rokonuzzaman *et al.* [15] defined a smart device in terms of ten basic attributes: environmental agility, autonomy, learning, real-time information processing, novelty, personality, ability to cooperate, two-way communication, upgradable, and visual appeal.

Table 2 shows the correspondence between the attributes describing the device smartness according to the two surveys we are talking about. The four attributes not included in the table (namely, novelty, personality, upgradable, visual appeal) provide a characterization of smart devices from the consumer point-of-view. Those attributes are not relevant from the perspective of the present study.

Table 2. Correspondence between [14] and [15]

Smart device according to [14]	Smart device according to [15]
Context awareness	Environmental agility
Connecting	Ability to cooperate, Two-way communication
Autonomous computing	Autonomy, Learning, Realtime information processing

4. RESULTS

In light of the considerations collected in the previous two sections, we are now able to assign the correct meaning to the term device in the four instances listed in section 1., namely: (IoT) device, Smart (IoT) device, (IoT) Edge device, and (IoT) Edge computing device. In the context of the cloud-only architecture, the term "(IoT) device" denotes the sensor (either passive or active) that collects the data from the surrounding physical environment and transmits it through the network to the cloud, where storage and processing take place. The other three terms are not applicable (NA).

With the advent of the Edge computing paradigm, the term "(IoT) device" has taken on the meaning of smart device, *i.e.*, this term denotes the pair: sensor(s)+MCU. At the same time, the remaining two terms were introduced (*i.e.*, "(IoT) Edge device" and "IoT Edge computing device"). The notion (Mobile) Edge computing device was firstly introduced in 2008 [37], in the context of large scale sensor networks.

Similarly, in the context of Edge AI the term "(IoT) device" should be attributed the declination of smart device according to [14] and [15]. While the remaining three terms maintain the same meaning that they have in the context of the Edge computing architecture. Table 3 summarizes what has been stated so far.

Table 3. Meaning of the four terms under investigation

Paradigm	The terms	Meaning of the term
Cloud-only	(IoT) device	Sensor
	Smart (IoT) device	NA
	(IoT) Edge device	NA
	(IoT) Edge computing device	NA
Edge-cloud	(IoT) device	Smart device
	Smart (IoT) device	Smart device
	(IoT) Edge device	Smart device
	(IoT) Edge computing device	Smart device
Edge AI	(IoT) device	Smart device
	Smart (IoT) device	Smart device
	(IoT) Edge device	Smart device
	(IoT) Edge computing device	Smart device

5. THREATS TO VALIDITY

This section addresses potential threats to the validity of the findings of this study, discussing internal, external, and conclusion validity. Internal validity measures the degree of confidence with which it is possible to state that the results from a study are conclusive and cannot be influenced by other factors. We investigated works published by ACM, Elsevier, IEEE, and Springer or indexed by Scopus; this method guarantees that the selected researches have been peer-reviewed before publication. Furthermore, having extracted works that cite "(IoT) device" either in the Title, in the Abstract, or as an Author' keyword is equivalent to basing our conclusions on studies focused on the IoT domain which, therefore, are relevant to build a map of the evolution of its meaning over the years.

External validity refers to the relevance of the results and their generalizability. About the relevance of the findings, the more the retrieved studies are relevant, the more the findings are relevant. To address this threat, we queried works published by ACM, Elsevier, IEEE, and Springer or indexed by Scopus. Such a choice guarantees that the selected researches have been peer-reviewed before publication. The generalizability of the findings of the study cannot be claimed given the goal of the research.

Conclusion validity refers to threats that can impact the reliability of the conclusions. The analysis and interpretation of the results were conducted considering 36 relevant studies spanning from 2004 to 2024. A potential threat might be caused by an incorrect interpretation of the concepts described in those papers. To mitigate this threat, all the articles were carefully reviewed.

6. CONCLUSION

Language grows and continuously adapts, evolving as we come up with better words that reflect our society or culture. In particular, it mirrors the complexity with which our lives intertwine with technology. When our technology evolves quicker than ever before, so too does our language. Because, as with technology, we strive to optimize language so we can communicate complex ideas, with the minimal amount of ambiguity in the most efficient way.

This study investigated the evolution of the concept of device in the IoT ecosystem, in the period spanning from 2004 to 2024. From the reading of a large number of Scopus studies, it emerged a direct relation between the evolution of the IoT computing paradigms and the meaning of the word device in the following commonly used four expressions: (IoT) device, Smart (IoT) device, (IoT) Edge device, and (IoT)

Edge computing device. Removing ambiguities in the interpretation of terms daily used by the IoT stakeholders is a precondition to improving the communication and cooperation among them.

ACKNOWLEDGEMENTS

Authors thank Professor Paolino Di Felice for the fruitful conversations during the entire journey of conceptualization and writing of this work.

REFERENCES

[1] Statista, “Number of internet of things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030,” *statista.com*, 2024. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (accessed Apr. 11, 2024).

[2] B. Dong, Q. Shi, Y. Yang, F. Wen, Z. Zhang, and C. Lee, “Technology evolution from self-powered sensors to AIoT enabled smart homes,” *Nano Energy*, vol. 79, Jan. 2021, doi: 10.1016/j.nanoen.2020.105414.

[3] “Microcontroller (MCU) Market. Report Code: 1084,” *Precedence Research*, 2023. https://www.precedenceresearch.com/press-release/microcontroller-market (accessed Apr. 10, 2024).

[4] O. Debauche, S. Mahmoudi, S. A. Mahmoudi, P. Manneback, and F. Lebeau, “A new edge architecture for AI-IoT services deployment,” *Procedia Computer Science*, vol. 175, pp. 10–19, 2020, doi: 10.1016/j.procs.2020.07.006.

[5] T.-W. Sung, P.-W. Tsai, T. Gaber, and C.-Y. Lee, “Artificial intelligence of things (AIoT) technologies and applications,” *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, Jan. 2021, doi: 10.1155/2021/9781271.

[6] I.-J. Ding and Y.-J. Chang, “HMM with improved feature extraction-based feature parameters for identity recognition of gesture command operators by using a sensed Kinect-data stream,” *Neurocomputing*, vol. 262, pp. 108–119, Nov. 2017, doi: 10.1016/j.neucom.2016.11.089.

[7] A. S. Syed, D. Sierra-Sosa, A. Kumar, and A. Elmaghraby, “IoT in smart cities: a survey of technologies, practices and challenges,” *Smart Cities*, vol. 4, no. 2, pp. 429–475, Mar. 2021, doi: 10.3390/smartcities4020024.

[8] H. M. K. K. M. B. Herath and M. Mittal, “Adoption of artificial intelligence in smart cities: a comprehensive review,” *International Journal of Information Management Data Insights*, vol. 2, no. 1, Apr. 2022, doi: 10.1016/j.jjimei.2022.100076.

[9] F. Firouzi, B. Farahani, M. Barzegari, and M. Daneshmand, “AI-driven data monetization: the other face of data in IoT-based smart and connected health,” *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 5581–5599, Apr. 2022, doi: 10.1109/JIOT.2020.3027971.

[10] S. Madderi Sivalingam and S. Thisin, “A new framework to enhance healthcare monitoring using patient-centric predictive analysis,” *International Journal of Electrical and Computer Engineering*, vol. 14, no. 3, pp. 3295–3302, Jun. 2024, doi: 10.11591/ijece.v14i3.pp3295-3302.

[11] V. P. Vemuri, Priya, V. R. Naik, V. Chaudhary, K. RameshBabu, and M. Mengstie, “Analyzing the use of internet of things (IoT) in artificial intelligence and its impact on business environment,” *Materials Today: Proceedings*, vol. 51, pp. 2194–2197, 2022, doi: 10.1016/j.matpr.2021.11.264.

[12] M. Achouch *et al.*, “On predictive maintenance in industry 4.0: overview, models, and challenges,” *Applied Sciences*, vol. 12, no. 16, Aug. 2022, doi: 10.3390/app12168081.

[13] M. S. Padmini and S. Kuzhalvaimozhi, “Critical analysis of life span improvement techniques in energy constraints Edge IoT devices,” *SN Computer Science*, vol. 4, no. 3, Feb. 2023, doi: 10.1007/s42979-022-01601-3.

[14] M. Silverio-Fernández, S. Renukappa, and S. Suresh, “What is a smart device? - a conceptualisation within the paradigm of the internet of things,” *Visualization in Engineering*, vol. 6, no. 1, Dec. 2018, doi: 10.1186/s40327-018-0063-8.

[15] M. Rokonuzzaman, K. (Kate) Kim, K. K. Dugar, and J. Fox, “What makes an object smart? Conceptualization, development, and validation of a scale to measure the smartness of a thing (SoT),” *Journal of Business Research*, vol. 141, pp. 337–354, Mar. 2022, doi: 10.1016/j.jbusres.2021.11.040.

[16] N. Gershenfeld, R. Krikorian, and D. Cohen, “The internet of things,” *Scientific American*, vol. 291, no. 4, pp. 76–81, Oct. 2004, doi: 10.1038/scientificamerican1004-76.

[17] F. Pereira, R. Correia, and N. Carvalho, “Passive sensors for long duration internet of things networks,” *Sensors*, vol. 17, no. 10, Oct. 2017, doi: 10.3390/s17102268.

[18] W. Kassab and K. A. Darabkh, “A–Z survey of internet of things: architectures, protocols, applications, recent advances, future directions and recommendations,” *Journal of Network and Computer Applications*, vol. 163, Aug. 2020, doi: 10.1016/j.jnca.2020.102663.

[19] C. C. Sobin, “A survey on architecture, protocols and challenges in IoT,” *Wireless Personal Communications*, vol. 112, no. 3, pp. 1383–1429, Jun. 2020, doi: 10.1007/s11277-020-07108-5.

[20] G. Paolone, D. Iachetti, R. Paesani, F. Pilotti, M. Marinelli, and P. Di Felice, “A holistic overview of the internet of things ecosystem,” *IoT*, vol. 3, no. 4, pp. 398–434, Oct. 2022, doi: 10.3390/iot3040022.

[21] A. A. Alli and M. M. Alam, “The fog cloud of things: a survey on concepts, architecture, standards, tools, and applications,” *Internet of Things*, vol. 9, Mar. 2020, doi: 10.1016/j.iot.2020.100177.

[22] M. S. Aslanpour, S. S. Gill, and A. N. Toosi, “Performance evaluation metrics for cloud, fog and edge computing: a review, taxonomy, benchmarks and standards for future research,” *Internet of Things*, vol. 12, Dec. 2020, doi: 10.1016/j.iot.2020.100273.

[23] F. Firouzi, B. Farahani, and A. Marinšek, “The convergence and interplay of edge, fog, and cloud in the AI-driven Internet of Things (IoT),” *Information Systems*, vol. 107, Jul. 2022, doi: 10.1016/j.is.2021.101840.

[24] O. Ali, M. K. Ishak, M. K. L. Bhatti, I. Khan, and K.-I. Kim, “A comprehensive review of internet of things: technology stack, middlewares, and fog/edge computing interface,” *Sensors*, vol. 22, no. 3, Jan. 2022, doi: 10.3390/s22030995.

[25] S. S. Gill, “A manifesto for modern fog and edge computing: vision, new paradigms, opportunities, and future directions,” in *Operationalizing Multi-Cloud Environments*, 2022, pp. 237–253.

[26] G. Rong, Y. Xu, X. Tong, and H. Fan, “An edge-cloud collaborative computing platform for building AIoT applications efficiently,” *Journal of Cloud Computing*, vol. 10, no. 1, Dec. 2021, doi: 10.1186/s13677-021-00250-w.

[27] F. Sakr, F. Bellotti, R. Berta, and A. De Gloria, “Machine learning on mainstream microcontrollers,” *Sensors*, vol. 20, no. 9, May 2020, doi: 10.3390/s20092638.

[28] T. Sipola, J. Alatalo, T. Kokkonen, and M. Rantonen, “Artificial intelligence in the IoT era: a review of edge AI hardware and software,” in *2022 31st Conference of Open Innovations Association (FRUCT)*, Apr. 2022, pp. 320–331, doi: 10.23919/FRUCT54823.2022.9770931.

[29] J. Zhou, S. Pal, C. Dong, and K. Wang, “Enhancing quality of service through federated learning in edge-cloud architecture,” *Ad Hoc Networks*, vol. 156, Apr. 2024, doi: 10.1016/j.adhoc.2024.103430.

[30] C. Min, A. Mathur, U. G. Acer, A. Montanari, and F. Kawsar, “SensiX++: Bringing MLOps and multi-tenant model serving to sensory edge devices,” *ACM Transactions on Embedded Computing Systems*, vol. 22, no. 6, pp. 1–27, Nov. 2023, doi: 10.1145/3617507.

[31] M. Merenda, C. Porcaro, and D. Iero, “Edge machine learning for AI-enabled IoT devices: a review,” *Sensors*, vol. 20, no. 9, Apr. 2020, doi: 10.3390/s20092533.

[32] N. N. Alajlan and D. M. Ibrahim, “TinyML: enabling of inference deep learning models on ultra-low-power IoT edge devices for AI applications,” *Micromachines*, vol. 13, no. 6, May 2022, doi: 10.3390/mi13060851.

[33] D. V. Tu, P. M. Quang, H. P. Nghi, and T. N. Thinh, “An edge AI-based vehicle tracking solution for smart parking systems,” in *International Conference on Intelligence of Things*, 2023, pp. 234–243.

[34] D. L. Dutta and S. Bharali, “TinyML meets IoT: a comprehensive survey,” *Internet of Things*, vol. 16, Dec. 2021, doi: 10.1016/j.iot.2021.100461.

[35] L. Capogrosso, F. Cunico, D. S. Cheng, F. Fummi, and M. Cristani, “A machine learning-oriented survey on tiny machine learning,” *IEEE Access*, vol. 12, pp. 23406–23426, 2024, doi: 10.1109/ACCESS.2024.3365349.

[36] A. Fanariotis, T. Orphanoudakis, K. Kotrotsios, V. Fotopoulos, G. Keramidas, and P. Karkazis, “Power efficient machine learning models deployment on edge IoT devices,” *Sensors*, vol. 23, no. 3, Feb. 2023, doi: 10.3390/s23031595.

[37] S. J. Kim, G. Deng, S. K. S. Gupta, and M. Murphy-Hoye, “Enhancing cargo container security during transportation: a mesh networking based approach,” in *2008 IEEE Conference on Technologies for Homeland Security*, May 2008, pp. 90–95, doi: 10.1109/THS.2008.4534429.

BIOGRAPHIES OF AUTHORS

Gaetanino Paolone received the Ph.D. degree in electrical engineering and information from the University of L’Aquila, Italy, in 2009. He is currently the CEO of B2B S.r.l. His research interests include software engineering, software development methodological processes, automatic code generation, artificial intelligence, and internet of things. He can be contacted at email: g.paolone@b2binformatica.it.

Francesco Pilotti received the master’s degree in classics from the Sapienza University of Rome, Italy, in 2015. He is currently employed as Researcher at Gruppo SI S.c.a.r.l. His research interests include artificial intelligence approaches, paradigms, and models. He can be contacted at email: f.pilotti@softwareindustriale.it.

Andrea Piazza received the bachelor’s degree in automotive engineering from the Politecnico of Torino, Italy, in 2023. He is currently employed as software analyst, designer and developer at B2B S.r.l. His research interests include software engineering and internet of things. He can be contacted at email: a.piazza@b2binformatica.it.