The present document is the submitted version of the paper.
The final and accepted version can be found at:
https://link.springer.com/chapter/10.1007/978-3-031-34171-7_8

Putting Intelligence into Things:

An Overview of Current Architectures

Maria Belesioti[1], Ioannis P. Chochliouros[1], Panagiotis Dimas[2],

Manolis Sofianopoulos[2], Theodore Zahariadis[3], Charalabos Skianis[3]

and Enric Pages Montanera[4]

[1*] Hellenic Telecommunications Organization (OTE) S.A.,

99 Kifissias Avenue, 15124 Maroussi-Athens, Greece

mbelesioti@oteresearch.gr; ichochliouros@oteresearch.gr:

[2] COSMOTE Mobile Telecommunications S.A., Athens, Greece

[3] Synelixis Solutions S.A., Chalkida, Greece

[4] Atos Research & Innovation, Madrid, Spain

Abstract: In the era of the Internet of Things (IoT), billions of sensors collect data from their environment and process it to enable intelligent decisions at the right time. However, transferring massive amounts of disparate data in complex environments is a challenging issue. The convergence of Artificial Intelligence (AI) and the Internet of Things has breathed new life into IoT operations and human-machine interaction. Resource-constrained IoT devices typically need more data storage and processing capacity to build modern AI models. The intuitive solution integrates cloud computing technology with AIoT and leverages cloud-side servers' powerful and flexible processing and storage capacity. This paper briefly introduces IoT and AIoT architectures in the context of cloud computing, fog computing and more. Finally, an overview of the NEMO [1] concept is presented. The NEMO project aims to establish itself as the "game changer" of AIoT-Edge-Cloud Continuum by bringing intelligence closer to data, making AI-as-a-Service an integral part of self-organizing networks orchestrating micro-service execution.

Keywords: Internet of Things (IoT); Artificial Intelligence (AI); AIoT; AIoT-Edge-Cloud.

1 Introduction

The rapid development and implementation of intelligent IoT, cloud and edge technologies have enabled various technological advances in different areas of life. The main goal of IoT technology is to simplify processes in various fields, increase the efficiency of systems (technology and/or specific processes) and, ultimately, improve the quality of life. Towards fulfilling this challenge, sustainability has become a vital issue for those who see the dynamic development of IoT technologies being able to provide various valuable benefits. However, this rapid development must be carefully monitored and evaluated from the sustainability perspective to “limit” harmful effects and ensure innovative use and limited world resources. Considering the strengths and weaknesses of IoT technology, this requires considerable research effort in the current sense. The present paper aims to contribute to understanding the impacts of the current technological advances related to sustainable corporate development in the IoT and edge computing era.

The era of the Industry 4.0 revolution begins with the development of intelligent sensors technology to integrate AI-based systems used in real-time applications [2]. Smart sensors are a topic that contributes to increased production and sales in various industries [3]. These advantages are especially evident when commercially available technologies are used effectively. Additionally, sensors may “react” differently in different environments. They can provide data of varying quality that can mislead the respective underlying model's decisions and lead to classification errors if the corresponding model needs to be more robust. AI-based systems designed to solve a single classification challenge are labor-intensive and costly; even a single misclassification scenario is costly in this scope. Cloud and edge computing are essential technologies in the computing continuum for efficient data management "closer to its source" rather than sending raw data to data-centres [4]. These trends, therefore, require a "shift" towards the technical and business convergence of the previously formally separated cloud, edge and IoT domains.

The Internet of Things fundamentally aims to change diverse sectors of our society and economy. However, realizing the vision of IoT requires data processing (stream, static, or both) in a "sweet spot" in the edge cloud continuum. Far-edge/sensors produce data and actuate; edge/fog consists of "heterogeneous intermediate devices" where data can be processed; cloud facilities deliver unlimited processing capabilities, while all of them jointly (and supported by resources/services/data orchestration) constitute the edge-cloud continuum. In this context, future IoT platforms will have to manage processes in multi-stakeholder, multi-cloud, federated and large-scale IoT ecosystems.

"Key" challenges are related to the fact that such platforms (encompassing operating systems, up to applications) will have to jointly leverage the continuous progress of multiple enabling technologies such as, for example, 5G/6G networking, privacy and security, distributed computing, artificial intelligence, trust management, autonomous computing, distributed/innovative applications, data management, etc. Moreover, they must facilitate intelligent (autonomous) orchestration of physical/virtual resources and tasks by realizing them at the “optimal location” within the considered ecosystem (e.g., closer to where data is produced). This implies that resource-aware, frugal AI is needed to facilitate self-awareness and decision support across the heterogeneous ecosystem. Finally, it is also imperative that resource management considers the carbon footprint of the ecosystem, uses data and tasks efficiently and also leverages multi-owner heterogeneous renewable energy sources.

The next section of the paper provides an overview of the related work in this field, while Sect. 3 explains the layers of the IoT and AIoT architectures. Section 4 refers exclusively to the framework of the ongoing NEMO EU-funded project, highlighting its specific concept and objectives. Finally, Sect. 5 concludes the scope of the paper.

2 Related Work

With the rapid development of technology, the number of IoT devices has increased dramatically. However, due to its limited resources, it can run out of capacity when processing computationally intensive and time-sensitive applications. As such, compute offloads that use cloud and network edge nodes for processing and analyzing data are emerging, so edge computing has recently started receiving much attention [5]. It supports cloud-like computing at the network edge by providing compute and network resources along the path between data sources and cloud data centres [6]. Fog computing [7] and mobile edge computing [8] are two well-known edge computing paradigms. Fog computing focuses on the infrastructure side and is typically deployed at the edge of the core network. Mobile edge computing, on the other hand, focuses on the mobile user side and is typically deployed within the wireless access network. To this respect, many offload algorithms for edge computing have been proposed with different offload criteria to fall into different offload algorithms.

Chen et *al.* focus on performance in terms of the average number of beneficial cloud computing users and the average amount of computational effort across the system [9]. They designed a distributed computing offload algorithm to improve the wireless access efficiency of computing offload in the mobile edge cloud computing environment. At the same time, many computational offload algorithms have been proposed to reduce service delays, including both network and computational delays. Using the Markov decision process, Liu et *al.* [10] formulated a power-constrained delay minimization problem for mobile edge computing systems and proposed an efficient one-dimensional search algorithm. Further on, Yang et *al.* proposed a Multi-Dimensional Search and Adjustment (MDSA) method for connecting computation partitioning and resource allocation to reduce the average delay of latency-sensitive applications on mobile edge clouds [11]. Youselfpour et *al.*, aiming to reduce service delay for IoT applications, proposed interesting delay-minimizing guidelines for fog-capable devices in [12]. Zhang et *al.* studied the problem of allocating computing resources in a three-tier IoT fog network [13], focusing on performance from a utility perspective.

At the same time, Liu et *al.* explored the appearing tradeoffs between latency and reliability in mobile edge computing offloading [14], while Li et *al.* researched the offloading problem related to heterogeneous real-time activities in fog systems as well as the resource allocation investigating the compromise between high throughput and high task completion rate [15].

3 Internet of Things (IoT) and AIoT Architectures

This section provides a brief overview of the overall IoT architecture and edge computing in terms of related paradigms. IoT technology acquires global perception in a ubiquitous connected environment using sensors, wired and wireless networks and cloud computing. The IoT architecture is widely recognized as a tri-tier, consisting of three layers, as indicated shown in the figure below; the respective layers are the perception layer, network layer and application layer (cf. Figure 1).

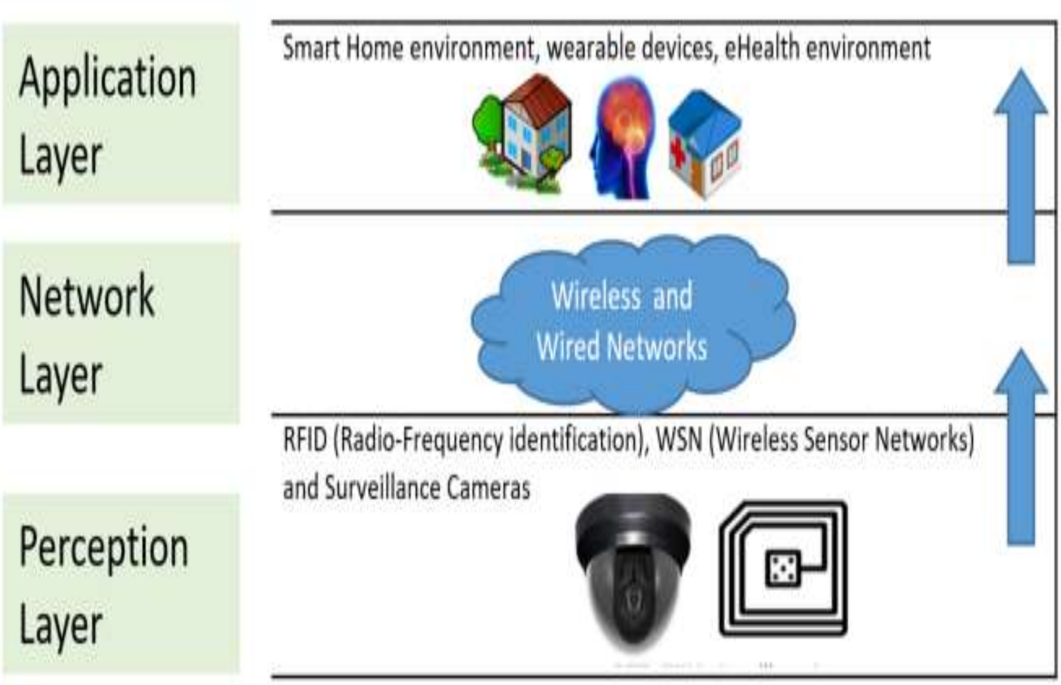
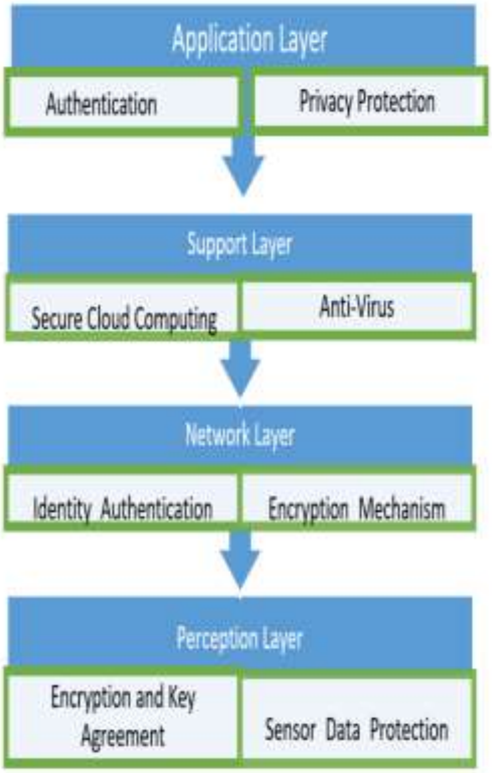


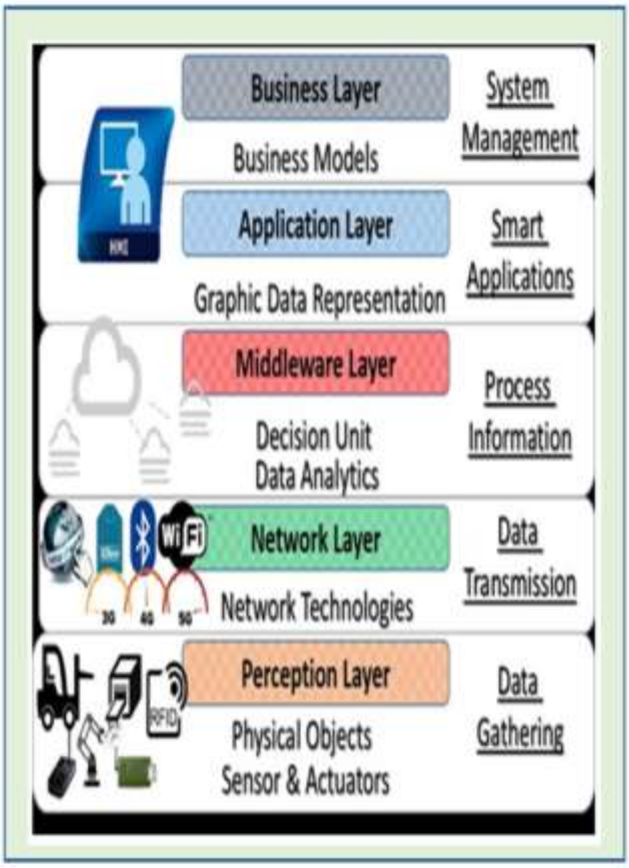
Figure 1: Three-layered architecture [16]

The perception layer, also known as the physical layer, includes diverse technologies and devices (such as sensors and actuators) according to the requirements of the intended applications per case. These devices are used for sensing and gathering information in the form of data, so that to enable comprehensive awareness of the surrounding environment(s). The network layer is the most standardized of the three IoT levels. Here, the devices existing at the perception level can communicate by using IoT gateways, wireless fidelity (Wi-Fi), Access Points (APs) and Base Stations (BS) for data transmission. The communication can be either short-range or long-range using various communication protocols such as, for example, Bluetooth, ZigBee, Sigfox, Long Range Radio (LoRa) and Narrowband IoT (NB-IoT). The data generated in the perception layer must be quickly and with accuracy transmitted to the server through the network layer and exactly. Within the application layer all the applications using IoT technology are defined. This layer can provide countless applications such as industrial control, urban management, smart agriculture and smart farming. This layer corresponds to the control level and the IoT decision layer.

However, the above three-tier architecture has been proved “insufficient” due to the fast-growing IoT requirements. Considering that, ITU-T [17] proposed a four-layer architecture introducing an additional layer, namely the support layer (also known as transport layer), between the network layer and the application layer (see Figure 2a).



(a)



(b)

Figure 2(a): Four- layer IoT Architecture [18];

(b): Five-layer IoT Architecture [19]

The new tier has been proposed because of the deficiencies in the 3-tier architecture and, more specifically, in order to enhance security in the architecture of IoT. In the prior approach, information is sent directly to the network layer of the three-tier architecture, so threats are more likely to appear. In the four-tier architecture, information is sent to the support layer and received by the perception layer. The support layer has two specific roles: to ensure the information is sent by genuine users and protected from threats. There are many ways to verify the authenticity of information. The most commonly used method is authentication, implemented with a pre-shared secret, key and password. The support layer's second task is sending information to the network layer. Radio- or wire-based is the medium for transferring information from the support layer to the network layer. Various attacks, such as Denial of Service (DoS) attacks, malicious insiders, and unauthorized access, can affect this layer [20].

The previously explained four-tier architecture has played an essential role in IoT development and approval. However, since security and storage issues continued, researchers have proposed a subsequent 5-layer architecture to secure the IoT [21]. Similar to previous architectures, there are three layers named perception layer, network layer, and application layer and two additional layers named middleware and business layers (cf. Fig.2b). This 5-tier proposed architecture meets multiple novel IoT technology requirements.

The processing layer, or the middleware layer, collects and processes the information sent by the network layer. Here, meaningless information is removed, and valuable information is extracted. This procedure solves the big data issue in the IoT domain since a large amount of information is received, thus impacting the IoT ecosystem's performance. The business layer is considered the "manager" of the system. The function of this specific layer is the management of IoT applications and intended services. Based on the volume of accurate data received from lower layers, it effectively analyzes such data. This layer can also determine how information is created, stored and modified, simultaneously managing t users' privacy.

3.1 Fundamentals of Artificial Internet of Things

The artificial intelligence of things is enabled by combining IoT [22] and artificial intelligence techniques [23]. IoT is defined as any device that can be interconnected – e.g. sensors – and collect data in real-time [24]. This relevance is revealed by processing the acquired data using artificial intelligence models, especially machine learning (ML) or, in some cases deep learning (DL), to analyze the collected data and extract valuable information for decision-making ([25], [26]).

Combining AI and IoT results in Artificial Intelligence of Things (AIoT) which, in turn, enables building more efficient IoT operations thus enhancing human-machine interaction and data management and analytics. IoT is considered the spine of the system, while artificial intelligence is the system's brain. AIoT is revolutionary and beneficial for both types of technology since artificial intelligence evaluates IoT through machine learning capabilities and IoT artificial intelligence through connectivity, signalling and data exchange. As IoT networks spread across large industries, there will be a large amount of human-centric, machine-generated data [27]. This can support data analytics solutions that can “add value’ to al data forms generated by IoT. Several IoT systems are designed for simple event control, but other events are much more complex, and IoT can be used for analytics purposes. AIoT elaborates on this context for preparing the appropriate steps to make this process happen. With intelligent tools on, edge devices are capable of observing their surroundings, perceiving data and finally making the best decision(s); and the most important is that all of these procedures can be implemented with the minor human intervention. Artificial intelligence transforms AIoT devices into intelligent machines capable of performing self-centred analysis and independent operations rather than mere messengers providing information to a control centre [28].

Regarding data analytics, with the combination of machine learning with IoT networks and systems, AIoT can create "learning machines." This can be applied to enterprise and industrial data, controlling IoT data such as the network edge and automating tasks in the connected workplace. Real-time data is critical to all AIoT applications and solutions. In particular, there are four main areas where AIoT is expected to have a significant impact: wearables, smart homes, smart cities and smart industry. Other fields are also currently expanding, requiring dynamic solutions that can be solved with AI, for example, sustainability [29], health [30], communication systems [31], data protection [32], electric vehicles [33] and power systems [34].

3.2 Overview of AIoT Architecture

Similar to IoT, AIoT also assumes a 3-tier architecture, this time from a computational perspective. The three layers are now cloud, fog and edge computing as illustrated in Figure 3.

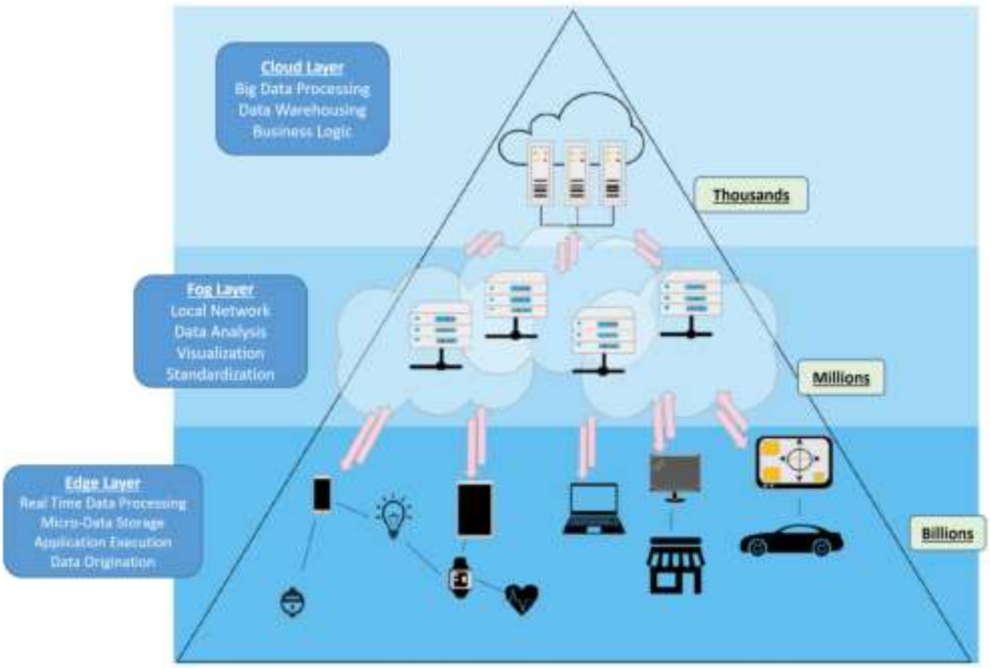


Figure 3: AIoT layered architecture [35]

The Edge computing layer can be considered as the perception layer in IoT architecture. It supports control and execution via sensors and actuators, enhancing AIoT systems' behavioural, overall perception and cognitive abilities. Fog computing is embedded in the fog nodes (i.e. hubs, routers, gateways) within the network; finally, the cloud computing layer supports application services per the IoT application layer. The fog and cloud computing layers have vast computational resources, access to considerable amounts of data and are primarily concerned with empowering AIoT systems with learning and reasoning capabilities.

3.2.1 Edge Layer

Edge networks are often powered by specific computing and storage capabilities. The bottom edge nodes are responsible for receiving data from the end devices of the perception layer and returning control flows to the devices over wireless interfaces [36]. The upper-edge servers use the received data to perform computational tasks, which, in cases of augmented complexity, can also be outsourced to higher-level servers with more powerful computational capabilities. Other edge server functions include authentication, authorization, offloading and storing data exchanged across the networks. This type of edge computing can reduce latency and provide continuous service while at the same time protecting data security and privacy. This has practical value for several AIoT applications such as agriculture, ships and smart grids where the internet could be more practically stable.

Edge layer resources are scarce compared to traditional cloud computing. This makes edge computing flexible and scalable, delivering various services anywhere between end-users and the cloud. Edge computing is usually viewed as an “extension” of cloud platforms and, in some scenarios, can work effectively, independently or in conjunction with cloud platforms. In this sense, edge computing refers to providing computing power to edge devices close to sensors and actuators. The emergence of edge computing depends on migrating computational tasks to the edge of the cloud, succeeding proximity to sensors or actuators, thus reducing the pressure of data transfer and the end-to-end (E2E) latency enabling real-time services. Here it should also be noted that fog and edge nodes are continuously distributed, while cloud nodes are not.

3.2.2 Fog Layer

The term “edge computing” is often confused with fog computing in literature [37] or is perceived as an “umbrella” term that includes fog as well. In fact, fog computing is responsible for bringing storage, computation, processing and networking capacity to the edge of the network, which is in the proximity of devices acting as an extension of and a ‘supplement” to cloud computing. Although fog nodes (routers, switches, gateways and wireless access points) are functioning similarly to cloud computing, fog computing can provide real-time collaborative services with less latency for numerous interconnected IoT devices as well as better data protection in terms of security and privacy since data can be held within the Local Area Network (LAN). Fog computing can provide real-time collaborative services with less latency for numerous interconnected IoT devices via distributed fog nodes [38].

3.2.3 Cloud Layer

The cloud enables AIoT corporations to have virtual computational resources instead of physical ones. The Cloud computing layer is a service-oriented architecture that provides flexible, scalable, elastic and reliable resources (such as computing, storage, and networking), enabling various AIoT applications and reducing information technology overhead for end-users and ownership costs. Real-time data is sent from distributed sensors and devices to remote cloud centres over the internet for processing and storage. However, cloud centres are usually built in remote locations far away from the end-user, thus causing delays in data transmission. With the increased number of IoT devices, the cloud cannot “meet” latency and data protection requirements, especially regarding latency-sensitive and privacy-sensitive applications [39]. AI can perform such tasks, and it is located in two places within an IoT ecosystem (i.e., centre and edge). AI deployments in centres traditionally generate predictive analytics or even anomaly detection. So far, AI deployments have mostly had a secondary function of reducing the amount of data entering the cloud.

4 NEMO Concept leveraging IoT

The Internet of Things can offer new and improved services and applications based on knowledge of the environment and the entities it contains. Millions of micro-suppliers could be created, formulating a highly fragmented market with new business opportunities able to offer commercial services. In this respect, the ongoing NEMO EU-funded project considers that intelligence needs to "move closer to the point of decision" and become an integral part of the AIoT meta-Operating System (mOS), supporting every activity, process and decision that ranges from ad-hoc micro-cloud cluster self-organization to micro-services migration and intent-based programming. To facilitate knowledge easily and almost without administrator instant deployment on any AIoT device, all mechanisms need to be integrated and connected, essential mOS tools and plug-ins installed as a (semi-)automated/standalone software package while ensuring interoperability, trust, cybersecurity and privacy.

Under this framework the NEMO project [1] aims to "drive" the IoT-Edge-Cloud continuum to the next generation by offering flexible, multi-path 5G/IoT connectivity and a lightweight micro-services' mesh migration/execution to ensure horizontal and vertical scalability. NEMO will pursue a close collaboration among semi-autonomous IoT nodes, IoT fog clusters, far-edge and near-edge cloud, and national and federated cloud infrastructures. Following a flexible collaboration model, new generation AIoT nodes will be equipped with intelligence to function in a semi-autonomous mode, reducing the latency and performing many complex operations locally without transporting raw data. Furthermore, federated on-device learning, data sovereignty, and trusted, explicitly attested (edge) cloud nodes will "bring" AI to environments with limited network coverage. The NEMO core functionality will be offered by an AI-based meta-Orchestrator, which will automatically, and in real-time, re-configure the mOS set-up at each node (either IoT, Edge, Cloud, ad-hoc or hybrid Clouds) so that the end-to-end federation operates optimally, matching the applications' Service Level Objectives (SLOs) and the policies set by the mOS administrators.

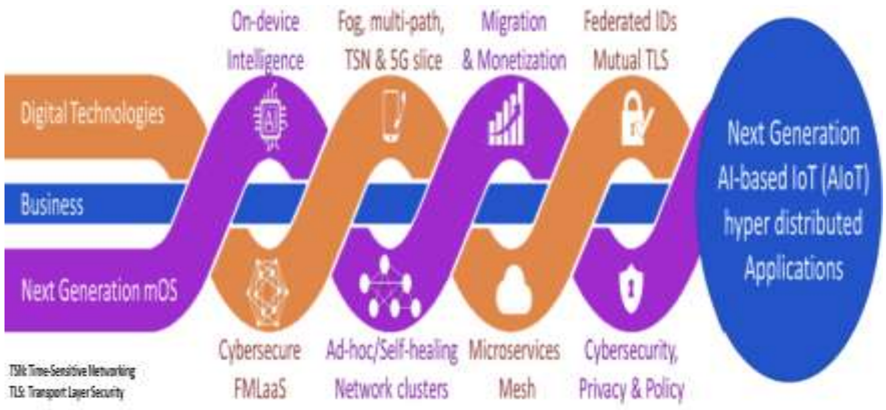


Figure 4. NEMO Concept

This effort will be highly related to security, regulation and legal restrictions. In this respect, new security and policy enforcement capabilities in the form of plug-in modules that comply with the terms of the Linux Security Modules (LSM) will be built for better protection against malicious code, cyberattacks or unintentional misconfigurations. Capabilities that go far beyond traditional smart contracts, such as data sharing and introducing innovative contractual perspectives as microservices, will consider the energy consumption and the costs of processing, storage, network/transmission, and cooling for providing optimal end-to-end services.

5 Conclusion

The Internet of Things is driving a significant transformation with the help of technologies such as 5G, fog computing and artificial intelligence to create new applications with specific requirements and greater flexibility and efficiency. This paper surveyed on several fundamental concepts (including IoT, AI and edge computing) and how these have managed to move the frontiers of AI away from the cloud network edge. Guided by these concepts, the paper also explores the general AIoT architecture and the integration that facilitated the corresponding rapid development. Connecting Edge Computing, IoT, and AI creates a new paradigm for edge intelligence with specific vertical industries such as smart agriculture, smart energy management, smart media and cultural experiences to exploit this innovative feature, also emphasizing the integration of substantial new data streams from machines and sensors.

This paper has so provided a comprehensive insight into the IoT and AIoT architectures, being able to promote on-edge intelligence. Specifically, first, our work has presented a short review of the related background and then the most known architectures. Based on these concepts, the paper has further outlined open challenges and future directions of AIoT in the context of the NEMO concept, aiming to have direct impact on several use cases of market importance.

Acknowledgements. Part of this paper has been based on the context of the "NEMO" ("*Next Generation Meta Operating System*") Project. This project has received funding from the EU Horizon Europe research and innovation Programme under Grant Agreement No.101070118.

References

[1]. NEMO, Horizon EU- funded project, GA No.101070118, https://meta-os.eu/

[2]. Peres, R.S., Jia, X., Lee, J., and Sun, K.A.W.J.: "*Industrial Artificial Intelligence in Industry 4.0 - Systematic Review, Challenges and Outlook*." *IEEE Access* 8, 220121--220139 (2020), https://doi.org/10.1109/ACCESS.2020.3042874

[3]. H. Ramamurthy, H., Prabhu, B.S., Gadh, R., and Madni, A.M.: "*Wireless Industrial Monitoring and Control using a Smart Sensor Platform*." *IEEE Sensors Journal* 7(5), 611--618 (2007) https://doi.org/10.1109/JSEN.2007.894135

[4]. *"The European Cloud, Edge and IoT Continuum Initiative*" (2023) https://eucloudedgeiot.eu/the-eu-vision-on-the-cei-continuum/

[5]. Shi W., and Dustdar, S.: "*The Promise of Edge Computing*." *Computer* 49(5), 78--81 (2016), doi: 10.1109/MC.2016.145.

[6]. Shi, W., Cao, J., Zhang, Q., Li, Y., and Xu, L.: "*Edge Computing: Vision and Challenges*." *IEEE Internet of Things Journal* 3(5), 637--646 (2016)

[7]. Bonomi, F., Milito, R., Zhu, J., and Addepalli, S.: "*Fog Computing and its Role in the Internet of Things*." In: *Proceedings of the* ACM *1st Ed. of the MCC Workshop on Mobile Cloud Computing (MCC'12)*, pp.13-16. ACM (2012)

[8]. Abbas, N., Zhang, Y., Taherkordi, A., and Skeie, T.: "*Mobile Edge Computing: A Survey*." *IEEE Internet of Things Journal* 5(1), 450--465 (2018)

[9]. Chen, X., Jiao, L., Li, W., and Fu, X.: "*Efficient Multi-user Computation Offloading for Mobile-Edge Cloud Computing*." *IEEE/ACM Transactions on Networking* 24(5), 2795--2808 (2016), https://doi.org/10.1109/TNET.2015.2487344

[10]. Liu, J., Mao, Y., Zhang, J., and Letaief, K.B.: "*Delay-optimal computation task scheduling for mobile-edge computing systems*." In: *Proceedings of the 2016 IEEE International Symposium on Information Theory (ISIT'16)*, pp.1451-1455. IEEE (2016)

[11]. Yang, L., Liu, B., Cao, J., Sahni, Y., and Wang, Z.: "*Joint Computation Partitioning and Resource Allocation for Latency Sensitive Applications in Mobile Edge Clouds*." In: *Proceedings of the 2017 IEEE 10th International Conference on Cloud Computing (CLOUD'17)*, pp.246-253. IEEE (2017)

[12]. Yousefpour, A., Ishigaki, G., and Jue, J.P.: "*Fog Computing: Towards Minimizing Delay in the Internet of Things*." In: *Proceedings of the IEEE International Conference on Edge Computing (EDGE'17)*, pp.17-24. IEEE (2017)

[13]. Zhang, H., Xiao, Y., Bu, S., Niyato, D., Yu, F.R., and Han, Z.: "*Computing Resource Allocation in Three-Tier IoT Fog Networks: A Joint Optimization Approach Combining Stackelberg Game and Matching*." *IEEE Internet of Things Journal* 4(5), 1204--1215 (2017)

[14]. Liu, J., and Zhang, A.Q.: "*Offloading Schemes in Mobile Edge Computing for Ultra-Reliable Low Latency Communications*." *IEEE Access* 6, 12825--12837 (2018)

[15]. Li, L., Guan, Q., Jin, L., and Guo, M.: "*Resource Allocation and Task Offloading for Heterogeneous Real-Time Tasks with Uncertain Duration Time in a Fog Queueing System*." *IEEE Access* 7, 9912--9925 (2019)

[16]. Mashal, I., Alsaryrah, O., Chung, T.Y., Yang, C.Z., Kuo, W.H., and Agrawal, D.P.: "*Choices for Interaction with Things on Internet and Underlying Issues*." *Ad Hoc Networks* 28, 68--90 (2015)

[17]. International Telecommunication Union – Telecommunication Standardization Sector (ITU-T): "*Recommendation Y4000/Y.2060 (06/12): Overview of the Internet of Things (2012)*", https://www.itu.int/rec/T-REC-Y.2060-201206-I

[18]. Burhan, M., Rehman, R.A., Khan, B., and Kim, B.-S.: "*IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey*." *Sensors* (MDPI) 18(9), 2796, https://doi.org/10.3390/s18092796

[19]. Antão, L., Pinto, R., Reis, J., and Gonçalves, G.: "*Requirements for Testing and Validating the Industrial Internet of Things*." In: *Proceedings of the 2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW'18)*, pp.110–115. IEEE (2018)

[20]. Sanzgiri, A., & Dasgupta, D.: "*Classification of Insider Threat Detection Techniques*." In: *Proceedings of the 11th Annual Cyber and Information Security Research Conference (CISRC'16)*, pp.1-4. ACM (2016).

[21]. Sethi, P., and Sarangi, S.R.: "*Internet of Things: Architectures, Protocols, and Applications*." *Journal of Electrical and Computer Engineering* 1--25 (2017), https://doi.org/10.1155/2017/9324035

[22]. Viel, F., Silva, L.A., Valderi Leithardt, R.Q., and Zeferino, C.A.: "*Internet of Things: Concepts, Architectures and Technologies*." In: *Proceedings of the 2018 13th IEEE International Conference on Industry Applications (INDUSCON'18),* pp.909–916. IEEE (2018),https://doi.org/10.1109/INDUSCON.2018.8627298

[23]. Sopelsa Neto, N.F., Stefenon, S.F., Meyer, L.H., Bruns, R., Nied, A., Seman, L.O., Gonzalez, G.V., Leithardt, V.R.Q., and Yow, K.-C.: "*A Study of Multilayer Perceptron Networks Applied to Classification of Ceramic Insulators Using Ultrasound*." *Applied Sciences* 11(4) 1592 (2021), https://doi.org/10.3390/app11041592

[24]. Leithardt, V., Santos, D., Silva, L., Viel, F., Zeferino, C., and Silva, J.: "*A Solution for Dynamic Management of User Profiles in IoT Environments*." *IEEE Latin America Transactions* 18(7), 1193--1199 (2020), doi: 10.1109/TLA.2020.9099759

[25]. Stefenon, S.F., Kasburg, C., Nied, A., Klaar, A.C.R., Ferreira, F.C.S., and Branco, N.W.: "*Hybrid Deep Learning for Power Generation Forecasting in Active Solar Trackers*." *IET Generation Transmission and Distribution* 14(23), 5667--5674 (2020)

[26]. Kasburg, C., Stefenon, S.F.: "*Deep Learning for Photovoltaic Generation Forecast in Active Solar Trackers*." *IEEE Latin America Transactions* 17(12), 2013--2019 (2019)

[27]. Guo, T., Yu, K., Aloqaily, M., and Wan, S.: Constructing a prior-dependent graph for data clustering and dimension reduction in the edge of AIoT. Future Generation Computer Systems **128**, 381--394 (2021)

[28]. Xiong, Z., Cai, Z., Takabi, D., and Li, W.: "*Privacy Threat and Defense for Federated Learning with Non-i.i.d. Data in AIoT*." IEEE *Transactions on Industrial Informatics* 18(2) 1310--1321 (2022), doi:10.1109/TII.2021.3073925.

[29]. Muniz, R.N., Stefenon, S.F., Buratto, W.G., Nied, A., Meyer, L.H., Finardi, E.C., Kühl, R.M., de Sá, J.A.S., and da Rocha, B.R.P.: "*Tools for Measuring Energy Sustainability: A Comparative Review*." *Energies (MDPI)* 13(9), 2366 (2020), https://doi.org/10.3390/en13092366

[30]. da Silva, L.D.L., Pereira, T.F., Leithardt, V.R.Q., Seman, L.O., and Zeferino, C.A.: "*Hybrid Impedance-Admittance Control for Upper Limb Exoskeleton Using*

Electromyography." *Applied Sciences (MDPI)* 10(20), 7146 (2020), https://doi.org/10.3390/app10207146

[31]. Kaur, J., Khan, M.A., Iftikhar, M., Imran, M., and Emad Ul Haq, Q.: "*Machine Learning Techniques for 5G and beyond*." *IEEE Access* 9, 23472--23488 (2021).

[32]. Lopes, H., Pires, I.M., Sánchez San Blas, H., García-Ovejero, R., and Leithardt, V.: "*PriADA: Management and Adaptation of Information Based on Data Privacy in Public Environments*." *Computers (MDPI)* 9(4), 77 (2020), https://doi.org/10.3390/computers9040077

[33]. Pinto, H., Américo, J., Leal, O., and Stefenon, S.: "*Development of Measurement Device and Data Acquisition for Electric Vehicle*." *Revista Gestão Inovação e Tecnologias* 11(11), 5809--5822 (2021), https://doi.org/10.7198/geintec.v11i1.1203

[34]. Stefenon, S.F., Furtado Neto, C.S., Coelho, T.S., Nied, A., Yamaguchi, C.K., and Yow, K.-C.: "*Particle swarm optimization for design of insulators of distribution power system based on finite element method*." *Electrical Engineering* 104, 615--622 (2022), https://doi.org/10.1007/s00202-021-01332-3

[35]. Permutive (2023), https://support.permutive.com/hc/en-us/articles/360012435279

[36]. Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J., and Lv, W.: "*Edge Computing Security: State of the Art and Challenges*." *Proceedings of the IEEE* 107(8), 1608--1631 (2019), https://doi.org/10.1109/JPROC.2019.2918437

[37]. Abbas, N., Zhang, Y., Taherkordi, A., and Skeie, T.: "*Mobile Edge Computing: A Survey*." *IEEE Internet Things Journal* **5**(1), 450--465 (2018), https://doi.org/10.1109/JIOT.2017.2750180

[38]. Bonomi, F., Milito, R., Natarajan, P., and Zhu, J.: "*Fog Computing: A Platform for Internet of Things and Analytics*." In: Bessis, N., Dobre, C. (eds), Big Data and Internet of Things: A Roadmap for Smart Environments. *Studies in Computational Intelligence* 546, 169--186 Springer, Cham (2014), https://doi.org/10.1007/978-3-319-05029-4_7

[39]. Zhou, Z., Chen, X., Li, E., Zeng, L., Luo, K., and Zhang, J.: "*Edge Intelligence: Paving the Last Mile of Artificial Intelligence with Edge Computing*." *Proceedings of the IEEE* 107(8), 1738--1762 (2019), https://doi.org/10.1109/JPROC.2019.2918951