FinJeHeW Finnish Journal of eHealth and eWelfare

SCIENTIFIC PAPERS

VERTAISARVIOITU
KOLLEGIALT GRANSKAD
PEER-REVIEWED
www.tsv.fi/tunnus

# Distributed network and service architecture for future digital healthcare

Erkki Harjula, Tanesh Kumar, Johirul Islam, Muneeb Ejaz, Ivana Kovacevic

Centre for Wireless Communications – Networks and Systems, University of Oulu, Oulu, Finland

**Erkki Harjula, Centre for Wireless Communications – Networks and Systems, University of Oulu, P.O. Box 4500, FI-90014 University of Oulu, FINLAND. Email: erkki.harjula@oulu.fi**

## Abstract

According to World Health Organization (WHO), the worldwide prevalence of chronic diseases increases fast and new threats, such as Covid-19 pandemic, continue to emerge, while the aging population continues decaying the dependency ratio. These challenges will cause a huge pressure on the efficacy and cost-efficiency of healthcare systems worldwide. Thanks to the emerging technologies, such as novel medical imaging and monitoring instrumentation, and Internet of Medical Things (IoMT), more accurate and versatile patient data than ever is available for medical use. To transform the technology advancements into better outcome and improved efficiency of healthcare, seamless interoperation of the underlying key technologies needs to be ensured. Novel IoT and communication technologies, edge computing and virtualization have a major role in this transformation. In this article, we explore the combined use of these technologies for managing complex tasks of connecting patients, personnel, hospital systems, electronic health records and medical instrumentation. We summarize our joint effort of four recent scientific articles that together demonstrate the potential of the edge-cloud continuum as the base approach for providing efficient and secure distributed e-health and e-welfare services. Finally, we provide an outlook for future research needs.

**Keywords:** health technology, telemedicine, cloud computing, internet of things, remote sensing

## Introduction

Following the recent and foreseen development in wireless communication and computing technologies, such as 5G, Internet of Things (IoT), Edge computing, Artificial Intelligence (AI), Machine Learning (ML) and Distributed Ledger Technologies (DLT), a wide variety of novel services will be enabled in the near future [1]. Healthcare is one of the application domains that will greatly benefit from this development, drawing keen interest from the industry, the research community and the public sector [2]. At the same time, the aging population and the growth of chronic diseases will cause huge pressure on the efficacy and cost-efficiency of healthcare systems, underlining the need for novel services and applications to streamline care pathways, thus making the healthcare personnel's work more efficient, as well as reducing the need for patients to travel to reach the necessary medical services. Furthermore, the resource efficiency – including energy-efficiency – are important factors for promoting cost-efficiency and sustainability of healthcare systems [3,4]. According to this justification, several technical challenges, related to e.g. ensuring performance, efficiency, reliability, security, privacy and system-level scalability, need to be addressed when adopting novel technologies [1,5].

In the digital transition of healthcare systems, Internet of Medical Things (IoMT), plays a significant role. It refers to the connected infrastructure of medical devices, software applications, systems and services. In IoMT systems, sensor information is gathered from a rapidly growing number of typically wirelessly connected low-power sensor devices, capturing patients' health data, such as heart rate, blood pressure, oxygen saturation, ECG or EEG [6]. Furthermore, IoMT helps to integrate data from medical imaging technologies, such CT, MRI and PET scanners with the rest of the IoMT system, allowing accurate real-time diagnostics. In addition, IoMT helps automating the patient treatment through e.g. remotely controlled infusion pumps, oxygen ventilators, smart beds, etc.

In most of today's solutions, data processing, storage, application logic and algorithms are handled at cloud data centers [7]. However, this centralized architecture is becoming problematic from the viewpoint of scalability, since novel IoMT devices generate high data volumes to be carried by networks, and to be processed and stored by data centers [1]. Another important challenge is related to the communication performance – latency in particular – and vulnerability for network problems, due to high physical and logical distance between the end-nodes and the server. These aspects pose a serious challenge for real-time and mission-critical applications, such as intensive care patient monitoring or computer-assisted surgery, which both require low latency and high reliability [8].

Furthermore, in healthcare applications, a particular concern is related to preserving the privacy and security of the patient data, and critical – even life-maintaining – system functions [1,5]. Centralized cloud systems are an inherently challenging environment from the viewpoint of security and privacy, since all data needs to pass several links and nodes, owned by a wide set of stakeholders between end-devices and data centers, not forgetting the chance for data leaks at data centers [1,5]. Therefore, the need for technologies, allowing secure and privacy-preserving data management and decision-making close to the data sources and the ability to control the scope of data propagation, is obvious [9].

## Technology background

**Internet of Medical Things (IoMT):** IoMT enables many key healthcare applications, such as remote patient monitoring, smart ambulance, portable medical imaging devices and secure sharing and maintenance of Electronic Health Records (EHR) [6]. Despite the advances in IoMT, there are still several open challenges to be addressed for future healthcare systems. For example, one of the major issues for IoMT is themanagement of the heaps of patient's data in delay-critical healthcare applications, requiring real-time data processing, analysis and decision-making. In addition, an important question is how different resources can be intelligently and efficiently utilized to fulfil the dynamic needs of various devices. Moreover, the security and data privacy are among the forefront requirements for future smart healthcare applications [10]. The emergence of various enabling technologies such as edge computing, virtualization, AI/ML and Blockchain (BC), among others, will empower the future IoMT-enabled mission and delay-critical healthcare applications.

**Edge computing (EC):** In traditional cloud systems, data-processing and storage, decision-making logic and different algorithms are handled at data centers. Many modern healthcare applications, however, require high Quality of Service (QoS), resilience to network problems, scalability and resource-efficiency, all of which cannot be fully satisfied by the centralized cloud model [11,12]. To overcome this challenge, EC has been introduced to bring cloud computing capabilities closer to the end-devices and data sources. EC can provide several desired features for IoMT scenarios, such as pre-processing and filtering of raw data in proximity of their sources to improve performance, reduce network burden and to avoid unnecessary propagation of private health data [13,14]. However, the current two-tier EC model, where EC hosts are deployed at servers, located within or near the access network base stations, also has its limitations [1]. In medical applications, at least some part of the processing would be optimal to be managed locally on site, to deal with possible connectivity problems, to utilize the available local computational capacity, and to reduce the access network load. Local IoMT clusters cannot, however, be expected to include devices with sufficient stability and capacity to accommodate a full-functional edge server, and, therefore, alternative decentralized solutions are needed [15]. For this, we have proposed a three-tier Edge IoT architecture, utilizing serverless edge computing model, which enables cloud functions to be deployed locally in a distributed virtualized manner [1,15]. The proposed model enables local deployment of e.g., critical IoMT services that require high availability and real-time functionality.

**Lightweight virtualization:** Virtualization technologies have revolutionized the world of software development and service design. Cloud-based service systems consist of application components that run on virtualized platforms distributed over multiple machines [16]. In these systems, traditional hypervisor-based virtualization solutions have provided a good level of isolation on a single hardware system, but also introduced significant overhead [17]. Container technologies, such as Docker and Linux container (LXC) systems, are developed to eliminate such overhead by packing software components and required resources into a single container image running on a single application on top of the host operating system [17,18], which helps increasing the processing speed of container instructions. Furthermore, in large virtual systems, such as cloud, the maintenance of complex and dynamic service ecosystems needs to be accommodated using orchestration technologies. Orchestration technologies, such as Docker Swarm and Kubernetes, provide functions such as dynamic service discovery, load balancing, and software upgrades [19].

**Distributed service technologies:** Cloud services were previously designed as monolithic applications associating multiple software components into a single entity. Monolithic service structures are, however, challenging to maintain and scale as the complexity of the system increases. Therefore, the current trend is towards a microservice paradigm, where service architectures consist of small, self-contained virtual components, microservices [19,20]. Microservices are typically based on containers that are relatively easy to develop in isolation and maintain as standalone software. Due to high granularity and ease of maintenance, several benefits, e.g., continuous development, scalability and failure tolerance, can be achieved. Function as a service (FaaS) [21,22] is a concept to execute modular software functions, at the edge. FaaS functions are small logical units that become alive when needed, then execute, and terminate when not needed anymore. Since FaaS functions typically do not run for long periods and their size is small, they do not necessarily require dedicated servers, and can instead be deployed on any device providing sufficient computational capacity, and therefore FaaS enables serverless computing. In this approach, data is processed by computationally capable local devices rather than being sent to a central location for processing. The processing tasks are split into smaller pieces and deployed to IoT devices in an efficient manner. In [1], we have named these pieces as “nanoservices”.

**Lightweight security, privacy and trust:** Healthcare systems are prone to a number of security threats at various levels, i.e., during transmission, sharing, storage and access of data [23]. The existing security approaches developed for current IoT architectures, however, are not well suited for local edge computing due to lower available capacity for execution and deployment [24]. Therefore, lightweight cryptography-based protocols [25], as well as efficient, adaptive and lightweight end-to-end security mechanisms are needed throughout the healthcare processes. Modern healthcare IoT systems consist of various involved stakeholders, such as patients, medical experts, hospital administration, laboratories, as well as infrastructure and service and software component providers. Establishing and maintaining trust between them is crucial in order to incentivize different stakeholders to share data with and use services from other stakeholders. DLT and its subclass BC emerge as promising candidates for building trusted distributed computing environments [26]. DLT and BC technologies establish a digital system for recording transactions of assets, where the transaction details are recorded in multiple places at the same time. Each node processes and verifies every item, thereby generating a record of each item and creating a consensus on its veracity. Furthermore, tracking and monitoring functionalities are enabled at various phases of processes to enhance the overall QoS [27]. By using DLT and BC technologies, various involved stakeholders and entities can securely share critical data and restrict access control to the authorized entities only.

## Concept

Due to their high potential for boosting the development of future digital healthcare applications, we have studied the feasibility of EC, virtualization and DLT/BC technologies in the healthcare context. Instead of repeating the convincing results found in the literature showcasing the generic benefits of these technologies – such as improved latency, higher reliability and ability to generate trust among distributed actors – *the aim of our work for this paper has been to study the practical technical implications and potential challenges on using these technologies in parallel for healthcare use, as well as proposing solutions how to maximize benefits while minimizing drawbacks*. Our centric key performance indicators (KPIs) are related to performance, resource-efficiency and energy-efficiency.

We have taken the concept called *edge-cloud continuum*, as a base approach for implementing the computational and communication architecture for future digital healthcare scenarios. The evolution of the Cloud IoT architecture is presented in *Figure 1,* where *1a* illustrates the traditional Cloud IoT architecture, *1b* depicts the current 2-tier

Edge-Cloud IoT architecture, and *1c* outlines the three-tier Edge-Cloud IoT architecture, on which we found our edge-cloud continuum concept. Our three-tier Edge-Cloud architecture [1], enables utilizing the most suitable – with respect to e.g. performance, reliability or efficiency – of the three architectural tiers for deploying different system components, namely *core tier* including traditional cloud data centers, *access tier* accommodating edge servers providing e.g. low latency, and *local tier* accommodating local edge machines capable of running the most lightweight edge services.

In [1], we also proposed a nanoservice-based conceptual service model, *nanoEdge (Figure 2a),* for future local Edge-IoT scenarios. The model takes EC a step forward from a typical today's Multi-Access Edge (MEC)-based architecture by providing needed mechanisms to deploy lightweight edge services to local nodes with sufficient hardware capacity. The proposed service model allows addressing problems, such as high latencies and vulnerability to network problems arising from long distances between computation, data sources, and service consumers. In nanoEdge model, local services are composed of modular, independent virtual service blocks, nanoservices, that can be dynamically deployed to local nodes with sufficient resources and stability for running them. A nanoservice typically contains a simple function implemented for a single purpose, such as reading sensor data from a device and sending it forward, or running a data analysis task and returning a response. In dynamic environment, the deployment can be modified based on the availability of nodes and resources, e.g., when new devices become available, existing devices become unavailable, or devices' load statuses change. This principle follows the Function-as-a-Service (FaaS) [21,22] and Serverless Computing models [15]. A Proof-of-Concept evaluation for the model was made in [28].

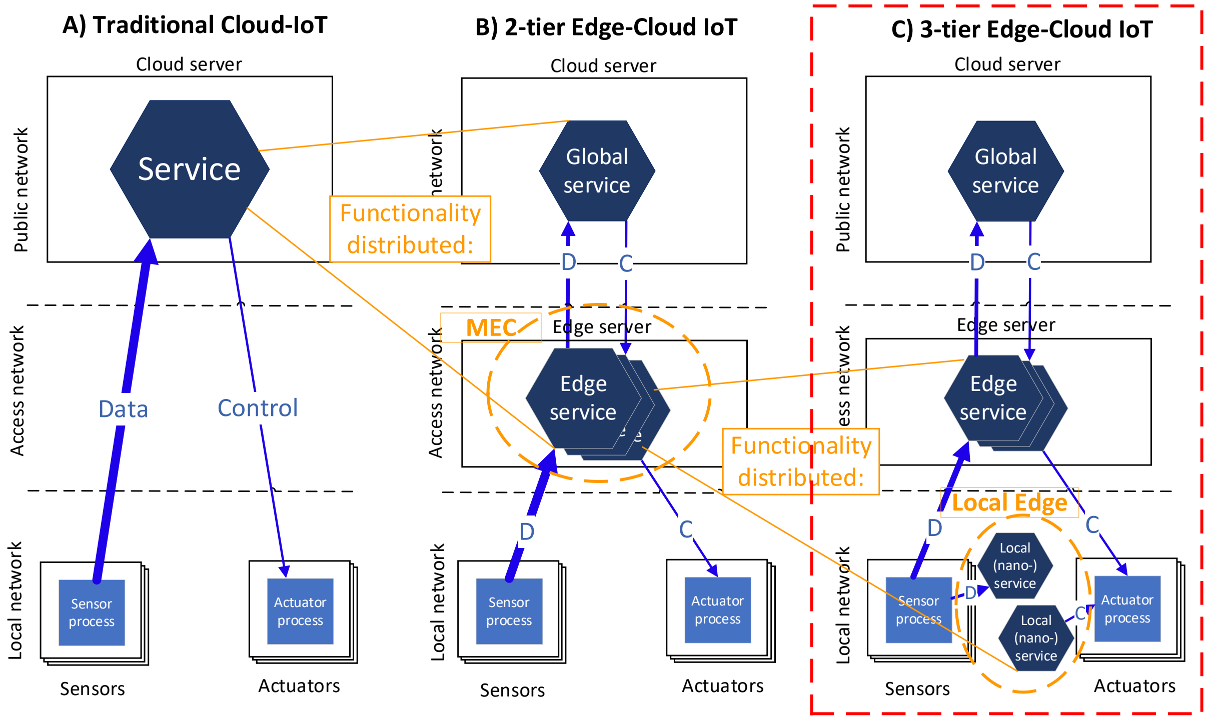
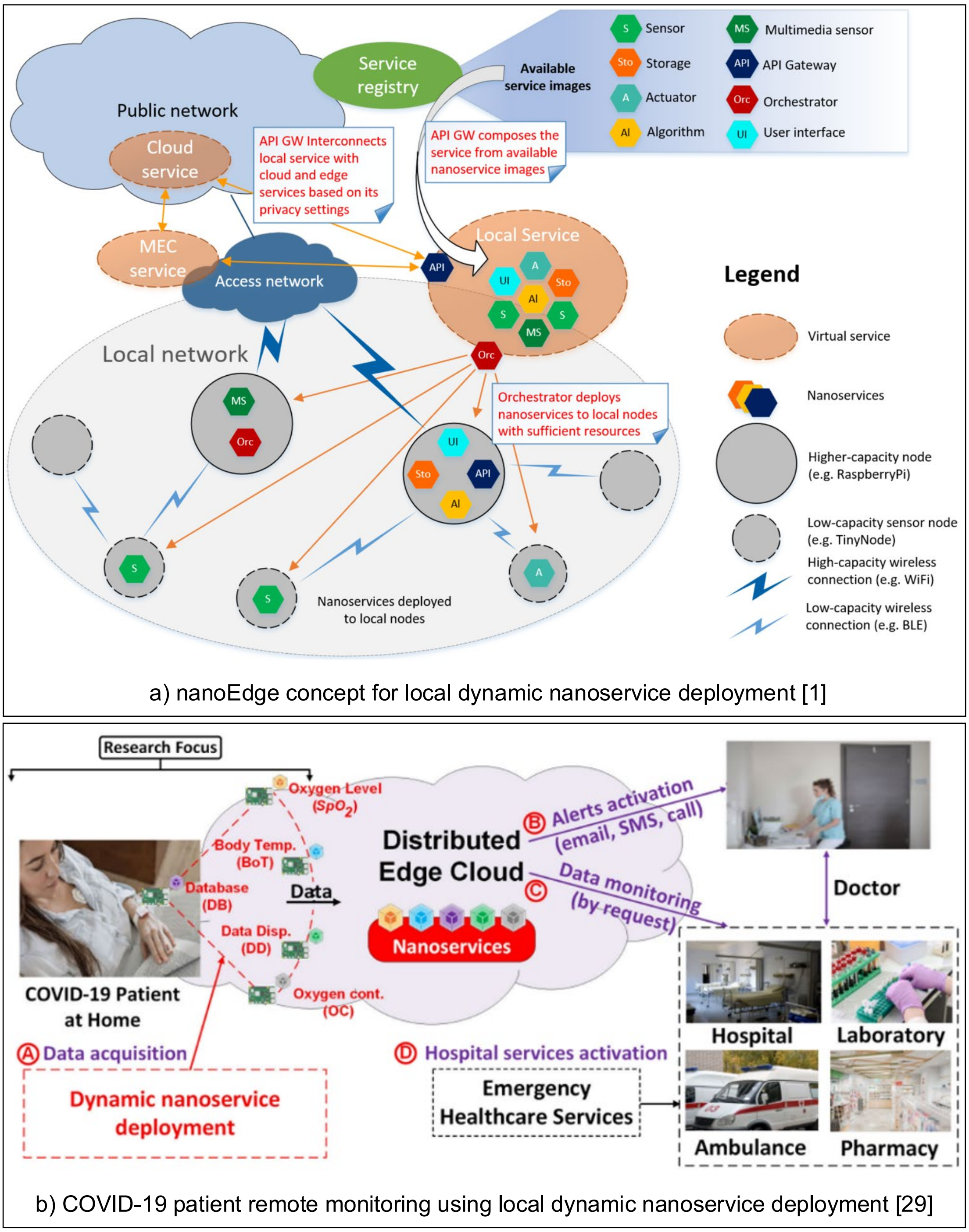


**Figure 1.** Cloud IoT architecture evolution.


Service registry
Available service images
S Sensor
Sto Storage
A Actuator
AI Algorithm
MS Multimedia sensor
API API Gateway
Orc Orchestrator
UI User interface
Public network
Cloud service
API GW Interconnects local service with cloud and edge services based on its privacy settings
API GW composes the service from available nanoservice images
MEC service
Access network
Local Service
Local network
Orchestrator deploys nanoservices to local nodes with sufficient resources
Nanoservices deployed to local nodes
Legend
Virtual service
Nanoservices
Higher-capacity node (e.g. RaspberryPi)
Low-capacity sensor node (e.g. TinyNode)
High-capacity wireless connection (e.g. WiFi)
Low-capacity wireless connection (e.g. BLE)
Research Focus
Oxygen Level (SpO2)
Body Temp. (BoT)
Database (DB)
Data Disp. (DD)
Oxygen cont. (OC)
Data
COVID-19 Patient at Home
Distributed Edge Cloud
Nanoservices
Ⓑ Alerts activation (email, SMS, call)
Ⓒ Data monitoring (by request)
Doctor
Hospital
Laboratory
Ambulance
Pharmacy
Ⓐ Data acquisition
Dynamic nanoservice deployment
Ⓓ Hospital services activation
Emergency Healthcare Services

a) nanoEdge concept for local dynamic nanoservice deployment [1]

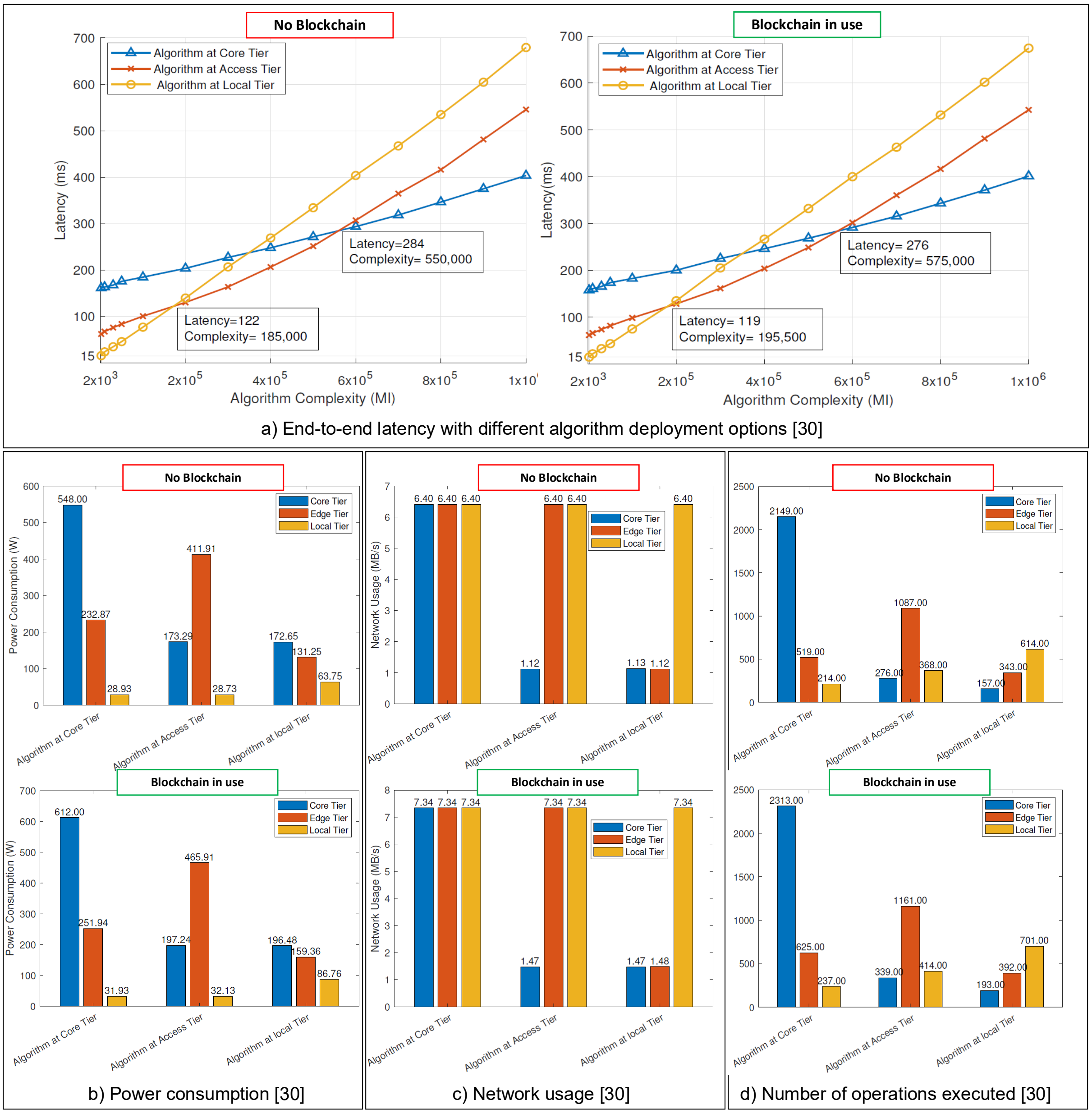
b) COVID-19 patient remote monitoring using local dynamic nanoservice deployment [29]

**Figure 2.** nanoEdge concept and remote patient monitoring use case.

## Concept validation

We have evaluated the feasibility of our concept with a series of real-world and simulation studies. In the following subsections, we briefly introduce these studies and their results, as well as discuss the significance of the results from the viewpoint of digital healthcare use cases.

**Local edge service orchestration:** In [29], we implemented a dynamic resource/service matching mechanism for distributed local EC. It extends our nanoEdge model by enabling automatic resource discovery and deployment in highly dynamic IoT scenarios, where the population of local nodes changes fast. To showcase the feasibility of the mechanism in real-life, we took Covid-19 patient monitoring as a use case for evaluations, where we measured the computational and communication latency of nanoservice deployment at each phase of the service deployment, and the storage capacity used by each nanoservice (*Figure 2b*). We were particularly interested on the extra latency introduced by the proposed virtualized (containerized) approach, compared to traditional non-virtualized approach, where functions were directly deployed on the underlying hardware. Virtualization ensures more efficient use of system resources, particularly in highly dynamic scenarios with nodes joining and leaving the cluster, as well as easy upgradeability. Therefore, the containerized approach was clearly a more favorable option for nanoservice deployment from the functional viewpoint. According to the results, virtualization adds 1-1.5 seconds (10-15%) extra latency in service deployment, while it reduces the worker node storage footprint from 35 MB to 23 MB (33%) and manager node storage footprint from 110-112 M to 96-98 MB (12-13%). Since container-based deployment has significant benefits in terms of e.g. better upgrading mechanism, scalability, self-healing, etc. minimal downtime, additional 1-2 seconds in the deployment phase are considered tolerable. Furthermore, reduced storage footprint allows more functionalities to be deployed on worker nodes. Overall, the deployment times and hardware requirements were seen feasible in the simulated treatment path, where a remotely monitored Covid-19 patient is transported from home to hospital after the system has detected deteriorating condition of a patient. Along the treatment path, the nanoEdge model enables gradual extension of a monitoring service to a treatment service, where e.g., an intelligent oxygen mask at ambulance could automatically connect to the SpO2 sensor of a patient brought to the ambulance and start regulating oxygen for a patient based on continuous measurement. Similarly, when moved to a hospital, the patient treatment service would be further extended with hospital instrumentation.



a) End-to-end latency with different algorithm deployment options [30]

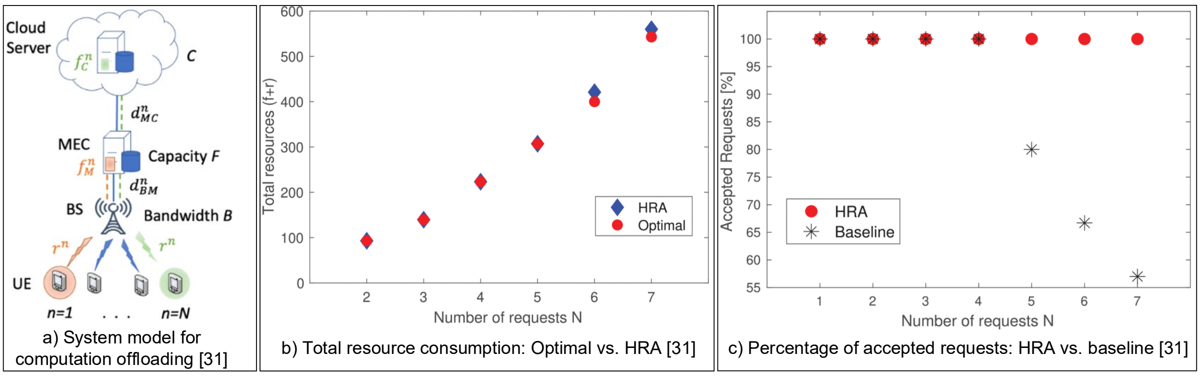
b) Power consumption [30]

c) Network usage [30]

d) Number of operations executed [30]

**Figure 3.** Blockchain edge architecture – measurement results.

**Blockchain edge architecture:** In [30], we studied the integration of BC with EC for enabling secure and trusted distributed telemedicine services. The proposed approach improves data privacy protection by 1) limiting the propagation of sensitive data instead of sending all data to the cloud, and 2) enabling the local anonymization of data that need to be sent for processing at public servers. With this approach, data leakage risks can be minimized by reducing the sensitive data to be sent out, while the consequences of possible data leaks can be mitigated by removing the real identities from patient data. We made simulations of data processing algorithms with different complexity classes in three deployment scenarios: a) traditional cloud-IoT scenario, (*Figure 1a*) where the application logic and algorithm were both deployed on a cloud data center; b) two-tier cloud-IoT scenario (*Figure 1b*), where the main application logic was still at a cloud data center, but the algorithm was deployed on an edge server co-located with a cellular network base station; and c) three-tier cloud-IoT scenario (*Figure 1c*), which was otherwise similar to scenario b, but the algorithm was deployed on a local device. All scenarios were run with and without BC data preprocessing, to reveal its burden on system performance and resource-efficiency. The evaluation results (*Figure 3*) revealed that the use of EC can effectively reduce the network burden on higher tiers with all scenarios, while from the end-to-end latency viewpoint, the optimal tier of algorithm deployment depends on the algorithm complexity. Furthermore, we observed that improved privacy protection by BC can be achieved with tolerable cost on performance and resource-efficiency in all scenarios, when considering the achieved improvements in security, privacy, and trust in healthcare monitoring scenarios. In more detail, the use of BC pre-processing increased the overall power consumption by 10–20%, computational and communication overhead by 13–22%, and computational complexity by 10–15%, depending on which tier of operation the data analysis functions were deployed. Overall, the article demonstrated the feasibility of combined use of BC and EC to provide decentralized trust, reliable real-time access, and control of the communication/computational capacity in the digital healthcare environment, without compromising the system performance and resource efficiency.



a) System model for computation offloading [31]

b) Total resource consumption: Optimal vs. HRA [31]

c) Percentage of accepted requests: HRA vs. baseline [31]

**Figure 4.** Latency-aware edge computing offloading.

**Latency-aware edge computation offloading:** When orchestrating the service deployment of latency/mission-critical medical applications, such as surgical navigation, in the presence of limited local hardware resources, the task offloading decision between edge and cloud server should be made in a way that strict delay requirements are met. In [31], we formulated the joint optimization of communication and computation resources allocation for requests, which aims to minimize the usage of the resources while maximizing the number of accepted computation offloading requests. The system model is presented in *Figure 4a.* We proposed an efficient heuristic solution based on the single user optimal solution with the objective to minimize the usage of system resources, while maximizing the number of accepted latency-limited task requests. In practice, the purpose was to ensure the operation of latency/mission-critical medical applications in resource-constrained environments that may occasionally be under heavy load. Simulations were run to show the effectiveness of proposed algorithm compared to optimal and baseline solution where tasks are allocated according to different system parameters as they arrive. It is important to notice that, although in our scenarios, the local devices are wirelessly connected to the rest of the network, in many real-life medical scenarios the connection is wired. The features of different communication links (throughput, latency, reliability, energy-efficiency, etc.) will affect the offloading decisions, but it does not have effect on the feasibility of our offloading optimization model, since the access network capacity is just one of the parameters among many others (*Figure 4a*), affecting the outcome of the resource-aware orchestration. In the case of 5G connection, the link features are close to e.g. wired ethernet connection, whereas with earlier cellular generations, particularly the latencies are much higher. With different IoT communication technologies, such as BLE, ZigBee, etc., the capacity is, for one, radically lower compared to today's cellular and wired networks. With respect to communication link reliability, the wired links are, as a rule of thumb, more reliable, but in larger-scale networks, the routing structure is typically the most error-prone element due to e.g. network congestion. The results of [31] revealed that our solution gives allocations that are optimal or very close to optimal (*Figure 4b*) and that it outperforms the benchmark algorithm in terms of the acceptance rate (*Figure 4c*). The results demonstrate that our task offloading algorithm enables execution of computational tasks with strict delay requirements, which is necessary for delay-critical medical services. Minimizing the usage of resources per request allows higher resource utilization rate and therefore helps reducing the infrastructure costs and power consumption. Furthermore, thanks to improved resource utilization, our algorithm helps improving the scalability of the system, which is especially important in large and multi-site hospitals or other healthcare organizations.

## Conclusions and future work

In our recent work, we have successfully demonstrated the feasibility of the edge-cloud continuum as the base approach for providing efficient and secure distributed e-health and e-welfare services. This article summarizes the key results of our four recent scientific articles and interprets their significance for healthcare use. As the base architecture, we took a three-tier Edge-Cloud architecture [1], which enables utilizing the optimal of the three architectural tiers for deploying different system components. We started by introducing our conceptual nanoEdge service model for enabling efficient distributed local edge computing. Then we presented the results of our study related to dynamic resource-aware service orchestration [29] and the integration of Blockchain with Edge Computing for achieving sufficient level of privacy and trust between various stakeholders of distributed e-health and e-welfare services [30]. As the fourth contribution, we proposed and simulated an algorithm for edge-cloud orchestration to minimize the usage of system resources, while maximizing the number of accepted latency-limited task requests [31], which is especially important latency and mission-critical medical applications, such as surgical navigation.

Based on the 6G vision [32], we foresee that the focus of the technology development will be in integrating AI, ML, edge-cloud and distributed ledger technologies for enabling novel digital healthcare solutions and optimizing current solutions to be more effective, efficient and secure. Furthermore, besides the technology development, modeling and evaluating the costs and risks of developing current healthcare IT architecture towards the proposed direction is crucial. A comprehensive analysis of the current challenges and pitfalls in adopting the novel technologies to the daily processes of healthcare organizations, taking into consideration, e.g., the needed change management, the costs of transition and the regulatory requirements, is needed.

## Acknowledgements

This research work was supported by Academy of Finland, under the DigiHealth and 6G Flagship Projects (grants 326291 and 346208).

## Conflict of interest

No conflicts of interest.

## References

[1] Harjula E, Karhula P, Islam J, Leppänen T, Manzoor A, Liyanage M, Chauhan J, Kumar T, Ahmad I, Ylianttila M. Decentralized Iot Edge Nanoservice Architecture for Future Gadget-Free Computing. IEEE Access. 2019 Aug 21;7:119856-119872. https://doi.org/10.1109/ACCESS.2019.2936714

[2] Dang LM, Piran MJ, Han D, Min K, Moon H. A Survey on Internet of Things and Cloud Computing for Healthcare. Electronics. 2019;8(7):768. https://doi.org/10.3390/electronics8070768

[3] Pantzartzis E, Edum-Fotwe FT, Price ADF. Sustainable healthcare facilities: Reconciling bed capacity and local needs. Int J Sustainable Built Environment. Jun 2017;6(1):54-68. https://doi.org/10.1016/j.ijsbe.2017.01.003

[4] Schlomann B, Eichhammer W, Stobbe L. Energy saving potential of information and communication technology. Int J Decision Support Systems, Jan 2015:1(2):152-163. https://doi.org/10.1504/IJDSS.2015.067565

[5] Sezer OB, Dodgu E, Ozbayoglu AM. Context-aware computing, learning, and big data in internet of things: a survey. IEEE Internet of Things. Feb 2018;5(1):1-27. https://doi.org/10.1109/JIOT.2017.2773600

[6] Gatouillat A, Badr Y, Massot B, Sejdic E. Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine. IEEE Internet of Things. Oct 2018:5(5):3810-3822. https://doi.org/10.1109/JIOT.2018.2849014

[7] Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE commun surveys tuts. 2015;17(4):2347-2376. https://doi.org/10.1109/COMST.2015.2444095

[8] Zhang Q, Fitzek FHP. Mission Critical IoT Communication in 5G. In: Atanasovski V, Leon-Garcia A (eds). Future Access Enablers for Ubiquitous and Intelligent Infrastructures. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 159. Ohrid, Republic of Macedonia: Springer International Publishing; 2016. p. 35-41. https://doi.org/10.1007/978-3-319-27072-2_5

[9] Ylianttila M, Kantola R, Gurtov A, Mucchi L, Oppermann I. 6G White paper: Research challenges for Trust, Security and Privacy. arXiv:2004.11665. arXiv; 2020 [cited 17 Oct 2021]. https://doi.org/10.48550/arXiv.2004.11665

[10] Al-Turjman F, Nawaz MH, Ulusar UD. Intelligence in the Internet of Medical Things era: A systematic review of current and future trends. Computer Communications. 2020 Jan 15;150:644-660. https://doi.org/10.1016/j.comcom.2019.12.030

[11] Dong P, Ning Z, Obaidat M.S, Jiang X, Guo Y, Hu X, Hu B, Sadoun B. Edge computing based healthcare systems: Enabling decentralized health monitoring in Internet of medical Things. IEEE Network. 2020 Apr 30;34(5):254-261. https://doi.org/10.1109/MNET.011.1900636

[12] Awaisi KS, Hussain S, Ahmed M, Khan AA, Ahmed G. Leveraging IoT and Fog Computing in Healthcare Systems. IEEE Internet of Things. 2020 Jun 25;3(2):52-56. https://doi.org/10.1109/IOTM.0001.1900096

[13] Li X, Huang X, Li C, Yu R, Shu L. EdgeCare: Leveraging edge computing for collaborative data management in mobile healthcare systems. IEEE Access. 2019 Feb 8;7:22011-22025. https://doi.org/10.1109/ACCESS.2019.2898265

[14] Wei K, Zhang L, Guo Y Jiang X. Health monitoring based on internet of medical things: architecture, enabling technologies, and applications. IEEE Access. 2020 Feb 4;8:27468-27478. https://doi.org/10.1109/ACCESS.2020.2971654

[15] Cicconetti C, Conti M, Passarella A. A Decentralized Framework for Serverless Edge Computing in the Internet of Things. IEEE Transactions on Network and Service Management. 2020 Sep 10;18(2):2166-2180. https://doi.org/10.1109/TNSM.2020.3023305

[16] Sosinsky B. Cloud Computing Bible. 1st rev. Wiley Publishing; 2011. 528 p. https://doi.org/10.1002/9781118255674.ch1

[17] Morabito R. Virtualization on Internet of Things Edge Devices with Container Technologies: A Performance Evaluation. IEEE Access. 2017 May 17;5:8835-8850. https://doi.org/10.1109/ACCESS.2017.2704444

[18] Felter W, Ferreira A, Rajamony R, Rubio J. An updated performance comparison of virtual machines and linux containers. IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS); 2015. p. 171-172 https://doi.org/10.1109/ISPASS.2015.7095802

[19] Pahl C, Brogi A, Soldani J, Jamshidi P. Cloud Container Technologies: A State-of-the-Art Review. IEEE Transactions on Cloud Computing. 2019 Jul-Sep 1;7(3):677-692. https://doi.org/10.1109/TCC.2017.2702586

[20] Rodgers R. The Tao of Microservices. 1st rev. Manning Publications; 2017. 328 p.

[21] Kuhlenkamp J, Werner S. Benchmarking FaaS Platforms: Call for Community Participation. In: IEEE/ACM Int Conf on Utility and Cloud Computing Companion (UCC Companion); 2018. p. 189-194. https://doi.org/10.1109/UCC-Companion.2018.00055

[22] García López P, Sanchez-Artigas M, Paris G, Pons DB. Comparison of FaaS Orchestration Systems. IEEE/ACM International Conference on Utili-

ty and Cloud Computing Companion (UCC Companion); 2018. p. 148-153. https://doi.org/10.1109/UCC-Companion.2018.00049

[23] Pramanik PKD, Pareek G, Nayyar A. Security and privacy in remote healthcare: Issues, solutions, and standards. In: Jude HD, Balas VE (eds). Telemedicine technologies. Academic Press; 2019. p. 201-225. https://doi.org/10.1016/B978-0-12-816948-3.00014-3

[24] Amin R, Kumar N, Biswas GP, Iqbal R, Chang V. A lightweight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment. Future Gener Comput Syst. 2018 Jan;78(3):1005-1019. https://doi.org/10.1016/j.future.2016.12.028

[25] Kumar T, Braeken A, Jurcut AD, Liyanage M, Ylianttila M. AGE: authentication in gadget-free healthcare environments. Information Technology and Management. 2020;21:95-114. https://doi.org/10.1007/s10799-019-00306-z

[26] Zhao S, Li S, Yao Y. Blockchain enabled industrial Internet of things technology. IEEE Transactions on Computational Social Systems. 2019 Jul 9;6(6):1442-1453. https://doi.org/10.1109/TCSS.2019.2924054

[27] Kumar T, Ramani V, Ahmad I, Braeken A, Harjula E, Ylianttila M. Blockchain utilization in healthcare: Key requirements and challenges. IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom); 2018. p. 1-7. https://doi.org/10.1109/HealthCom.2018.8531136

[28] Islam J, Harjula E, Kumar T, Karhula P, Ylianttila M. Docker Enabled Virtualized Nanoservices for Local IoT Edge Networks. IEEE Conference on Standards for Communications and Networking (CSCN); 2019. p. 1-7. https://doi.org/10.1109/CSCN.2019.8931321

[29] Islam J, Kumar T, Kovacevic I, Harjula E. Resource-aware Dynamic Service Deployment for Local IoT Edge Computing: Healthcare Use Case. IEEE Access. 2021 Aug 5;9:115868-115884. https://doi.org/10.1109/ACCESS.2021.3102867

[30] Ejaz M, Kumar T, Kovacevic I, Ylianttila M, Harjula E. Health-BlockEdge: Blockchain-Edge Framework for Reliable Low-Latency Digital Healthcare Applications. Sensors. 2021;21(7):2502. https://doi.org/10.3390/s21072502

[31] Kovacevic I, Harjula E, Glisic S, Lorenzo B, Ylianttila M. Cloud and Edge Computation Offloading for Latency Limited Services. IEEE Access. 2021 Apr 8;9:55764-55776. https://doi.org/10.1109/ACCESS.2021.3071848

[32] University of Oulu. 6G Flagship - Discover how 6G will change our lives. Oulu: 6G Flagship, University of Oulu [cited 17Oct 2021]. Available from: https://www.oulu.fi/6gflagship/