Chapter 1

Healthcare Internet of Things: The State of the Art

The Internet of Things has the potential to change the world, just as the Internet did.

Kevin Ashton

This chapter presents an overview of the latest technological advancements in the healthcare Internet of Things (H-IoT) domain.

This work studies the opportunities offered by the most cutting-edge technologies to deal with challenges of H-IoT in the Communication layer. The following contents cover H-IoT's state of the art. First, section 1.1 presents the general H-IoT network's landscape in both software and hardware aspects. Second, section 1.2 describes our focused technology's emergence in the SOTA architecture in detail. Next, section 1.3 demonstrates our learned lessons and points out neglected opportunities offered by the network advancements for H-IoT, which later leads to our proposed solutions. We also position our research, define our concentration in this work, and present the prospects of our proposed solutions in this discussion. Finally, concluding this chapter, section 1.4 summarizes our findings and navigated directions.

1.1. H-IoT network landscape

In 1999, "Internet of Things" was first introduced by Kevin Ashton. The terminology describes a system in which objects in the physical world could be connected to the Internet by sensors. After more than 20 years of development history, IoT has become one of the crucial business market (Rejeb et al. 2022).

Along with the paradigm's advancements, a vital branch, H-IoT, has also progressed in the general IoT landscape, while sufficiently improving human life quality. Since it is a subset of the IoT paradigm, H-IoT architecture inherits the standard components in a general IoT architecture (Bouazizi et al. 2017; Elayan et al. 2017). Despite sharing common characteristics, Healthcare IoT also possesses some distinguish requirements compared to the generic IoT that specified by Qadri et al. (2020) in Table 1.1.

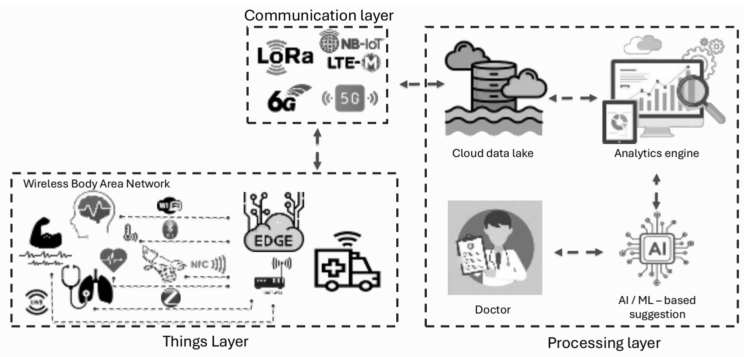

Figure 1.1. *Three-tier H-IoT architecture: Things, Communication and Processing layers. For a color version of this figure, see www.iste.co.uk/chu/softwaredefined.zip*

	Generic IoT	H-IoT
1	It is usually deployed over a large geographical area and serves a single purpose.	Usually deployed in a closed or small geographical area, either in and around the human body or in a healthcare facility.
2	Energy sources can include solar and wind energy. In case of stationary nodes, the nodes may be powered continuously.	H-IoT nodes can also harvest energy from human body using heat, stress and motion.
3	Monitor environment, used in defence applications, industrial monitoring.	Used to monitor human body vitals.
4	Desirably small nodes but node size vary according to environment and application.	The nodes are miniaturized to be unobtrusive.
5	Usually these are stationary.	Essentially mobile as associated with human body.
6	Deployment of sensors is comparatively easy.	Deployment is a difficult particularly in case of implants which mostly requires a surgery.
7	Data integrity is tried to maintain. The redundancy compensates for errors.	The data must be preserved and transmitted with utmost integrity.

Table 1.1. *Healthcare IoT and generic IoT comparision*

Besides identifying H-IoT's characteristics from general IoT, Qadri et al. (2020) also presented an abstract H-IoT communication architecture.

Inspired by their work, we update the general H-IoT architecture with the most recent advancements, such as the adoptions of 5G/6G, Cloud Data Lake and AI intervention in supporting Healthcare decision making, and illustrate these changes in Figure 1.1. The architecture still indicates the fundamental healthcare data flow as it consisted of three main layers: the Things, Communication and Processing layers.

Technology	Types	Frequency	Data Rate	Range	Power Usage
NFC	PAN	13.56 MHz	100–400 kbps	10 cm	Very Low
Bluetooth 4	PAN	2.4 GHz	1 Mbps	0.1 km	Low
Bluetooth 5	PAN	2.4 GHz	2 Mbps	0.25 km	Very Low
ISO/IEC 15693	PAN	3.56 MHz	6.6–26 Kbit/s	1–1.5 m	Very Low
Z Wave	LAN	968–908 MHz	100 kbps	100 m	Very Low
RFID	LAN	13.56 MHz–2.45 GHz	40–640 kbps	1–100 m	Low
Thread	LAN	2.4 GHz	250 Kbits/s	10–100 m	Low
Wi-Fi	LAN	2.4 GHz and 5 GHz	802.11(b)11 M; (g) 54 M; (n) 0.6; (Gac) 1 Gbps	50 m	Low–High
ZigBee	LAN	2.4 GHz	250 kbps	10–100 m	Very Low

Table 1.2. *Short range communication technologies parameters*

The Things layer collects the vital metrics generated by the sensing devices and then forwards those toward higher processing units (gateway, edge/fog node) for further processing. Since the sensing devices in the Thing layers operate close to the human body, any health-affected impact requires careful and standardized consideration. The devices' size, flexibility, and thermal output are crucially important for their implementation feasibility. With limited power, memory and computing capacity, the sensing devices required a gateway to contain the data and later transmit the collected data to the central server. Wired and wireless solutions have been developed over the years to transfer the collected data from the sensing devices to the gateway in the H-IoT branch. Initially, wired solutions have been developed and utilized on the human body in healthcare facilities and the laboratory environment. However, these solutions have disadvantages (Talpur et al. 2019) such as the amount of sensors' limitation and inconvenience placement on the body and causing barriers in data collection. Hence, they are only suitable for a few specific use cases.

On the other hand, wireless solutions also known as wireless body area networks (WBAN) resolved most aforementioned disadvantages. Besides, the technology's advancements also help to reduce the size of the sensing device's communication component. Thus, the sensing device could be easily integrated within the human body while allowing various vital metrics to be transmitted to the gateway over the air (Talpur et al. 2019). Furthermore, since the operational environment of WBAN is the human body, most WBAN communication technologies fall in the short-range communication category. Well-known WBAN technologies and their communication parameters are in Table 1.2 (Ahad et al. 2020). These characteristics are also the leading factors toward the dominance of WBAN technology in the Things layer in the H-IoT branch. After collecting the data successfully, the gateway could preprocess it to reduce the computing and network resources later or forward it directly to the Processing layer via the Communication layer. Such edge interventions provide real-time critical analysis and/or the fastest response, which are critical for the H-IoT use case.

After the preprocessing phase, the data continue its lifecycle and is transmitted to the Processing layer via the communication infrastructure. The gateway indeed requires a higher computing and power capacity and long-range communication technologies to transfer the data to the Processing layer.

Long-range communication technologies suitable for this purpose are presented in Table 1.3 (Ahad et al. 2020). Once the data pass through the Internet infrastructure and are handled by the central data center, the final processing at the Processing layer occurs. At the end of the data lifecycle, the computed results or any necessary instructions would be returned to the Things layer in the reverse direction, and a new data lifecycle begins.

Technology	Types	Frequency	Data Rate	Range	Power Usage
WiMAX	WAN	10–66 GHz	11–100 Mbs	50 km	High
LoRa	WAN	868/915 MHz	50 kbps	25 km	Low
LoRaWAN	WAN	Numerous	0.3–50 kbps	$2-5$ km (Urban) 15 km (Suburban) 45 km (rural)	Low
Sigfox	WAN	868/915 MHz	300 bps	50 km	Low
4G	WAN	700, 1700, 2800 MHz	Up to 12 Mbps	Up to 10 km	High
5 G	WAN	At Low Bands	Up to 3.6 Gbps	Up to 10 km	High
5G	WAN	At High Bands	10 Gbps	<1 km	High
(NB-IoT)	WAN	850 MHz	245 kbps	Up to 35 km	High
(EC-GSM IoT)	WAN	890 MHz	Up to 140 kbps	Up to 100 km	High
LTE-M (M1)	WAN	700, 1450–2200, 5400 MHz	0.144 Mbps	35 km	High

Table 1.3. *Long-range communication technologies parameters*

A highlight that should be noticed in Table 1.3 is 5G technology. Mentioning the decade science breakthrough, 5G is one of the best candidates for the spotlight. After years of being developed and standardized since its first practical trials (Morgado et al. 2018), 5G has been widely deployed all over the world. Indeed, the 5G's first highlight is enhanced mobile broadband (eMBB). Thanks to its incredible theoretical 10–30 Gbps data rate (Ahmad et al. 2023), a single 5G link speed overfulfills most challenging network requirements, including ultra high-definition video, video calling (Sudhamani et al. 2023) and extreme AR/VR (2.35 Gbps) (Mangiante et al. 2017). Hence, they allow for the feasibility of such applications in optimal operating environments. Massive machine type communication (mMTC) is 5G's second prospective advantage compared to 4G. The second advancement enables billions of smart devices to connect to the Internet (Attaran 2023). Along with eMBB, massive multi-input multi-output technology is exploited to increase the device deployment maximum density to 1 million devices/km^2 (Eswaran and Honnavalli 2023). Finally, ultra reliable and low-latency communications (uRLLC) is another crucial 5G signature feature. Its promised advancement is the minimal end-to-end latency, only 4 ms compared to 200 ms in 4G.

With such advantages, 5G has strengthened the IoT's wide adoption (Liu et al. 2018b) in various domains, and one of them is smart healthcare (Li 2019) or eHealth. In other words, 5G is a vital factor in recent H-IoT revolution (Ahad et al. 2020). As compliance in the state-of-the-art H-IoT architecture and worldwide 5G adoption, Ahad et al. (2020) presents one of the latest general H-IoT communication infrastructure architectures. Inspired by their work, we illustrate the cutting-edge H-IoT architecture in Figure 1.2 to highlight the device-to-device links, 5G's impact and emphasized the ambulance's role. Instead of describing the data flow like in Figure 1.1, this diagram indicates H-IoT hardware infrastructure and the interactions within the communication ecosystem. In addition to the Cloud computing infrastructure and medical care center being specified as the final destination in the Processing layer, various cellular technologies empower the communicating function for the Communication layer. Conversely, the people, ambulances, and Edge clouds act as the gateway endpoints in the Things layer. Besides, the device-to-device links also play a crucial role in inter-WBAN communication. Last but not least, the figure also presents a perspective of multi-hop metric transmission in the H-IoT domain.

Besides being a performance boosting factor to the Communication layer, 5G technology also unlocks a novel network management perspective to the public, which is network slicing (Barakabitze et al. 2020). Specifically, before 5G's existence, the community commonly delegates the infrastructure network management to the mobile network operators, Internet service providers, etc. There are two main reasons for this observation: the exclusive management of the industrial companies and the costly deployment and maintenance expenses of self-managed private networks. Network slicing in 5G, however, reshaped this network phenomenon. The core concept behind the paradigm will be discussed in detail in the next chapter. However, a point worth mentioning is the paradigm's inspiring impact. The slice concept offers the third-party actors to reflect their demands over their assigned overlay of a deployed network infrastructure. Therefore, a third party could operate their dedicated network overlay while the underlying network infrastructure are still maintained by the infrastructure providers. Thus, both aforementioned barriers are eliminated. Hence, 5G established a network perspective that enabled a plethora of opportunities for future research in the eHealth domain with an unconstrained hardware management landscape.

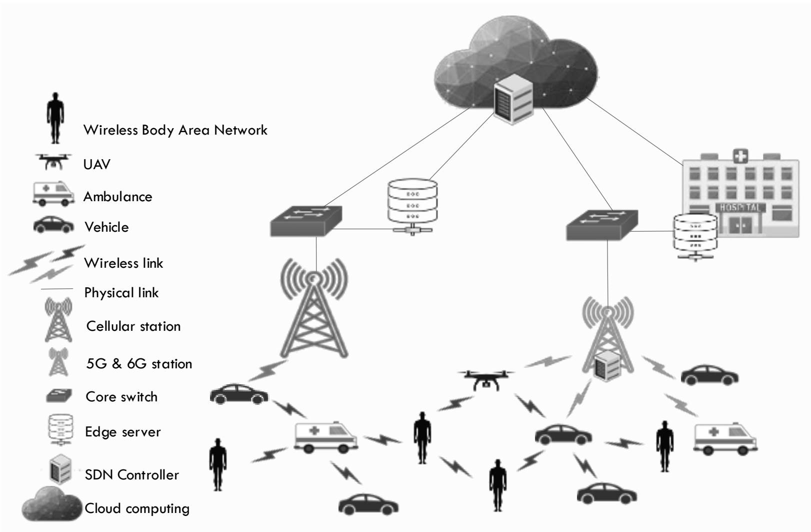

Figure 1.2. *H-IoT communication infrastructure. For a color version of this figure, see www.iste.co.uk/chu/softwaredefined.zip*

However, such promising prospects still require further effort to be achievable. One of the vital factors that held the community back in this direction is the limited number of network slices in the current 5G implementation. Despite numerous promising possibilities, only three slices are ready to use in 5G's implementation: eMBB, uRLLC and mMTC

(Popovski et al. 2018). Regarding their names, these slices' functions defined by the 3GPP standard are as follows. While eMBB slice aims to support a stable channel with high peak data rate, mMTC slice focuses on ensuring a massive number of IoT connections with small data payload. Last but not least, uRLLC allows 5G to achieve an ultra-low latency transmission (4 ms). Notably, each slice's objective is to satisfy a distinguished technical aspect defined by the infrastructure orchestrator. Hence, the specialized prospects for more complex and critical situations that require a mixture of the mentioned objectives still need to be clarified.

Correlated with this work, consider the crisis contexts or disaster scenarios as an example: eHealth communication is crucial to ensure the operation's success. However, since eHealth communication requires the most demanding communication specifications, it is vital to prioritize the medical task force's communication while maintaining average communication in such circumstances. Thus, constructing a temporary dedicated slice with a higher priority that satisfies eHealth communication constraints could be a feasible situational approach. Figure 1.3 is inspired by a use case of a 5G e-health slice in Thales' vision[1]. The figure illustrated the network-slicing vision of a customer's complex mixture requirements in a static industrial network infrastructure. First, it categorized three main layers in the network slicing concepts: tenant point-of-view; service orchestrators; and network infrastructure. Toward a unified hardware platform, the mobile transport and the hardware infrastructure perform the fronthaul and backhaul network integration between various infrastructure providers. On top of the common infrastructure, the slice orchestrator manages the united networking capability and computing resources to formulate network slices regarding

1 Presented by Emmanuel Dotaro, Head of ICT & Security labs, Thales/SIX/CTO, "5G basics and a bit beyond".

the customer's service-oriented specifications (mobile (virtual) network operator (MVNO), eHealth, automotive, media and entertainment). The slice orchestrator also provides a frontend, which serves as an entry point to support their tenant a service point-of-view for slicing creation and management requests. Even if the described prospect is practical, the current network slicing landscape is still tied to a predeployed network infrastructure. On the other hand, particularly in the eHealth domain, the infrastructure's integrity is uncertain in the mentioned challenging circumstances. A part or all of the existing infrastructure may malfunction or become unavailable because of the objective environmental causes (Khan et al. 2022) in such scenarios. Thus, a more versatile networking solution is expected to provide the communication capability for such time-critical situations. Once again, thanks to wireless communication advancements, flexible network coverage deployment is more feasible in the cutting-edge 5G network context. However, further investigation in this direction will be discussed in the next chapter. We have now provided the reader with the latest H-IoT network landscape. In the following discussion, we study the emergence of cutting-edge technologies in the H-IoT branch.

1.2. Technology emergence in H-IoT

After architectural-level and cutting-edge network landscape investigations, further discussions are emerging concerning the latest technologies in the H-IoT domain. The section aims to provide the audience with the overall landscape followed by this thesis navigation process before proceeding with our proposed contributions in the following chapters. To achieve this goal, we present two distinguished studies about our focused technology emergence in the H-IoT domain: multi-access edge computing and software-defined networks.

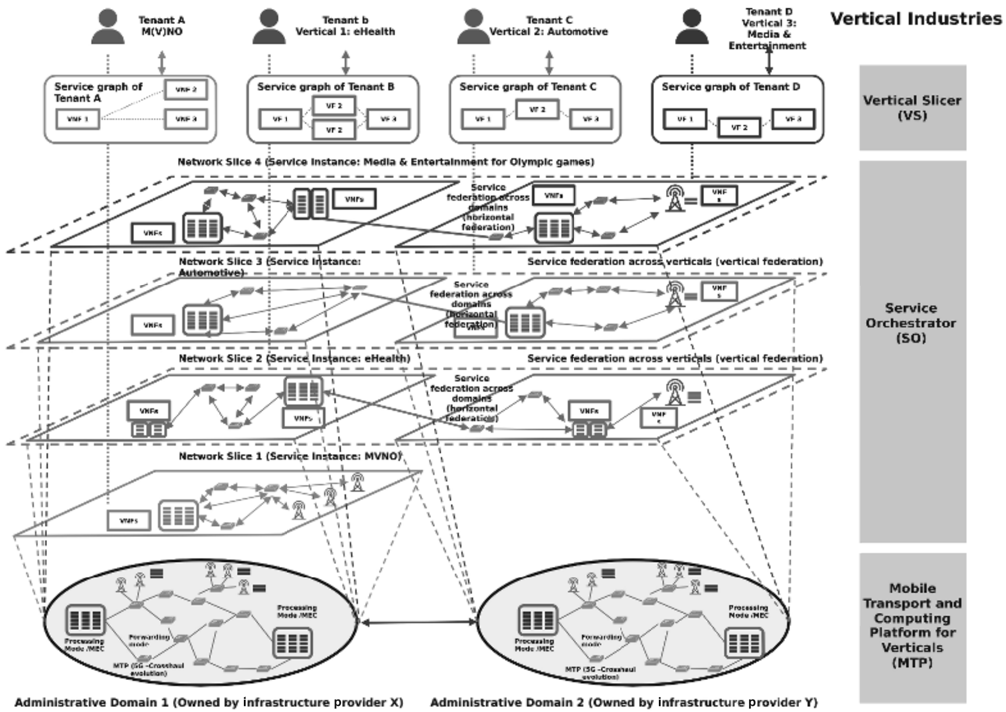

Figure 1.3. *eHealth dedicated slice technological landscape. For a color version of this figure, see www.iste.co.uk/chu/softwaredefined.zip*

1.2.1. *Edge computing in H-IoT*

1.2.1.1. *Cloud/fog/edge history*

Along with the described WBAN progression in the previous section, the cloud/fog/edge computing developments are another crucial enabling factor for the H-IoT domain. In 1990, the very first form of multi-access edge computing (Khan et al. 2019) paradigm was invented as content delivery network (CDN) (Dilley et al. 2002), which is about reducing the proximity between the end-users device and the web server. Then, in 2006, once Amazon promoted their Elastic Compute Cloud Service for the first time (Al-Dhuraibi et al. 2018), the cloud computing paradigm received massive attention from the researchers. In the middle of the cloud computing technology's embracing, Cisco introduced the fog computing (Hazra et al. 2023) paradigm in 2012 to cope with the cloud computing limitations (central bottleneck, long physical communication distance, etc.). Cisco's introduction not only effectively presented its technological edges to the community but also promoted an existing solution advantage, which is CDN. Later, the paradigm was justified, unified and named after its characteristic, which is now well known in the community under the terminology multi-access edge computing (MEC). Possessing a few crucial advantages, edge computing's broad adoption in the academic and the industry is inevitable, including in our focused domain, that is, H-IoT. The following discussion covers the edge computing paradigm's state of the art in H-IoT.

1.2.1.2. *Edge computing's taxonomy in H-IoT*

The first step to novel technology adoption in a domain is studying the domain's technological landscape at the architectural level. Various investigations in this direction have been published over the years.

In 2015, Ramalho et al. (2015) presented their progressive work toward the Multi-eHealth Cloud Service Framework

(MeCa). The novelty in this continuous work is migrating MeCa computing scenarios from the cloud environment to the fog/edge environment, highlighting the edge computing performance improvement.

To investigate this crucial advantage further, Vora et al. (2017) studied edge computing advantage in neurological treatment where real-time monitoring is essential. The authors presented an architecture to monitor patients with chronic neurological diseases and performed data clustering to detect anomalies before transmitting data to the destination.

Later, in 2018, Rais et al. (2018) proposed a four-tier architecture for a Healthcare monitoring system by integrating WBAN sensors, fog/edge computing, and cloud services, especially in an IPv6 environment. A small-scale testbed results confirmed the medical communication requirements satisfied by their proposed architecture.

Instead of the small-scale laboratory environment, Muhammed et al. (2018b) also presented a ubiquitous edge computing-based healthcare framework for smart cities. Various cutting-edge technologies are also adopted in this work, such as deep learning and big data, to provide a personalized healthcare networked experience. However, the infrastructure for such advancements could only be formulated with the edge computing paradigm. The results obtained from their proof-of-concept system confirms the efficiency in latency reduction (50% compared to traditional cloud-based healthcare system). The future work specified by the authors is improving the formulated framework's security, privacy, reliability and scalability.

Exploiting further the strategic position in the edge network of the intelligent gateway, Rahmani et al. (2018) investigated a range of high-level medical data processing services. Later on, their proof-of-concept implementation was adopted in several gateways to form an intermediary processing layer for an early warning healthcare monitoring system.

On the other hand, Greco et al. (2019) focused on medical data streaming tasks in the H-IoT context. The four-layer architecture's performance is also conducted by performing anomaly detection tasks in the REALDISP dataset with the latest technological framework. The obtained result confirmed the performance satisfaction of the designed system.

Meanwhile, Chen et al. (2018) explored the edge-based resource allocation strategy of the edge computing paradigm. The authors proposed an edge cognitive computing-based healthcare system. Taking advantage of computing resource allocations, the results, based on the data-driven cognitive approach at the edge, confirm the overall QoS improvement.

In addition to SOTA, Pace et al. (2018) developed a valid and inexpensive gateway solution for H-IoT. The two most significant advantages were the solution's capability to support multi-radio, multi-WBAN communication technologies and exploit both public and private Cloud platforms to guarantee the system's flexibility. Two case studies (factory workers and athletes training) were also defined for the evaluation phase.

Foreseeing LPWAN advantage in H-IoT deployment, Queralta et al. (2019) and Kharel et al. (2019) proposed an LPWAN edge computing based healthcare monitoring architecture. However, these two papers concentrated on different aspects. In Queralta et al. (2019), the authors focused on achieving high accuracy in a fall detection task and waiving the need to transmit raw data to cloud servers for online analysis in the proposed edge-intelligence integrated system. Meanwhile, Kharel et al. (2019) investigated physical connectivity metrics to ensure the feasibility of LPWAN-based H-IoT systems.

Toward combining (Pace et al. 2018) short-range with Queralta et al. (2019) and Kharel et al. (2019) long-range communication capacity, Wu et al. (2019) presented a hybrid H-IoT network system for industrial safety monitoring applications. Hence, a robust H-IoT hybrid solution, which employed the edge computing heterogeneous communication technology to reduce the latency and improve network performance, was conducted.

Considering the vast amount of data generated by the H-IoT monitoring system, Abdellatif et al. (2020) proposed an edge-computing architecture that provides efficient data delivery, namely, multimodal data compression and edge-based feature extraction for event detection. The studies investigated data distortion ratio, data classification accuracy and energy consumption to ensure the proposed architecture's short response time, efficient processing and minimal energy and bandwidth consumption. Not submitting a novel architecture, however, Satija et al. (2017) and Siddique et al. (2018) also showed their research interest in data filtering at the edge level. While Satija et al. (2017) viewed the problem from a classification point of view, Siddique et al. (2018) approached the problem via a data compression landscape. These studies confirmed the system's energy efficiency in transmitting acceptable quality data. Besides being concerned about qualified data transmission, Hayajneh et al. (2019) fulfilled the data protocol research gap. Their study was composed of three distinct algorithms toward three different protocol objectives. The channel assignment algorithm is for minimizing and avoiding interference. The gateway association algorithm aims to improve the connection's efficiency and security. Last but not least, their proposed routing metric is for constructing minimized delay and conserved power routes.

Along with communication architectural and general data processing contributions, a plethora of papers were conducted to study edge-computing IoT systems focusing on some specific health-based purposes. Specifically, they are diabetes detection (Priyadarshini et al. 2018; Devarajan et al. 2019; Abdel-Basset et al. 2020), chikungunya outbreak detection (Sood and Mahajan 2018), activity classification (Pham et al. 2018; Uddin 2019; Ram et al. 2019), Covid detection (Hegde et al. 2020), arrhythmia anomaly detection (Azimi et al. 2019), voice disorder (Muhammad et al. 2018a), skin region classification (Dai et al. 2019), stress-type classification (Priyadarshini et al. 2018) and food classification for diet assessment (Liu et al. 2018a). Since this chapter focuses on the complex H-IoT management aspect, we will not investigate this health-purpose specific direction in detail.

After the brief introduction to the state of the art, we refined the conducted knowledge and summarized it into our taxonomy in Figure 1.4 and Table 1.4.

1.2.2. *Software-defined network in H-IoT*

1.2.2.1. *Software-defined network history*

After investigating edge computing's emergence, we shift our focus to the next worth-mentioning emergence in H-IoT, that is, software-defined networks. If the edge computing paradigm represents the processing transition of Internet infrastructure (from cloud to fog then edge), the software-defined network is the representative of the Internet's management transition.

To have a clearer understanding of this particular transition, Vaniukov and Vaniukov (2023) may provide valuable insight into Internet's current operation. The article reports the enormous amount of money spent on IT infrastructure, which indicates how costly and complex to maintain and operate the Internet.

Reference	**Contribution category**	**Data type or data set**	**Main Objective of exploiting edge computing in healthcare IoT**	**Performance metric**	**ML-based approach**	**Use case**
Ramalho et al. (2015)	Framework	eHealth notification	Save energy, lower latency, avoid centralized penalties by Fog distributed computing	Received transmitted traffic, Energy consumption	NA	Alarm system for healthcare monitoring
Vora et al. (2017)	Framework, Implementation	Movement traces	Provide minimum delay to the queries	Response time, observed traffic, jitter, Energy consumption	K-mean , C4.5 decision tree	Patient monitoring system for ambient assisted living
Satija et al. (2017)	Signal quality classification	MIT-BIH arrhythmia, Physionet Physiological	Filter data and improve data quality, battery time of IoT devices, reduce the cloud server traffic load, bandwidth and treatment costs	Classification accuracy, computational time	NA	Continuous cardiac health monitoring
Rais et al. (2018)	Architecture, Implementation	Physiological	Reduce load and time bound	Delay	NA	Patient health monitoring in hospital environment
Jangra and Gupta (2018)	Framework	Time-series data	Lower power consumption on BAN	Energy consumption	NA	Real time healthcare monitoring

Reference	**Contribution category**	**Data type or data set**	**Main Objective of exploiting edge computing in healthcare IoT**	**Performance metric**	**ML-based approach**	**Use case**
Muhammad et al. (2018a)	Framework, implementation	Various dataset	Enhance network Quality of Service, reduce latency	Latency reduction ratio, energy, classification accuracy, root mean square error, mean absolute error	Deep neural networks	Mobile healthcare framework for health monitoring, disease monitoring and remote super vision of surgery
Chen et al. (2018)	Framework, implementation	Medical history, physiological health risk level	Improve Quality of Experience in emergency case	Overall QoS	NA	Resource redistribution base on health risk level
Rahmani et al. (2018)	Framework, implementation	Physiological	Exploit higher-level service at the edge: local storage; real-time local data processing; embedded data mining; etc. improve energy efficiency, performance, interoperability, security and reliablity	Early warning score, latency ratio, compression ratio, latency	NA	Massive remote health monitoring system
Siddique et al. (2018)	Data compression	Physiological	Save energy	Energy consumption, SNR, PRD, PPR	Dictionary learning	Arrhythmia detection

Reference	Contribution category	Data type or data set	Main Objective of exploiting edge computing in healthcare IoT	Performance metric	ML-based approach	Use case
Priyadarshini et al. (2018)	Stress type classification, diabetes prediction, assessing hyper-tension's risk	Various	Reduce latency, increase throughput	Memory utilization, Classifcation accuracy	Deep neural network	Health monitoring and predict the wellness stats
Muhammad et al. (2018b)	Voice disorder detection, treatment framework	Saarbrucken Voice Disorder	Reduce bandwidth consumption	Bandwidth consumption, detection and classification accuracy	Deep learning	Voice disorder detection and classification
Sood and Mahajan (2018)	Disease classification	Physiological environmental location	Quick response, improve healthcare service	Classification time and classification accuracy	J48 decision tree	Diagnose and prevent the outbreak of Chikungunya
Pham et al. (2018)	Activity classification	Posture	Provide real-time data access, reduce the transmitted data, improve battery life	Energy consumption, classification accuracy	Gradient-boosting decision tree	Integrate contextual information for remote health monitoring
Liu et al. (2018a)	Food classification	UEC-256 Food 101	Recognize food for dietary assessment	Recognition accuracy, response time, energy consumption	CNN	Dietary assessment

Reference	Contribution category	Data type or data set	Main Objective of exploiting edge computing in healthcare IoT	Performance metric	ML-based approach	Use case
Dai et al. (2019)	Skin region classification	HAM10000	Reduce latency, improve privacy, lower cost	Classification accuracy	CNN	Detection and prevention of various diseases
Greco et al. (2019)	Framework, implementation	REALDISP	Quick response to anomalies	CPU usage, DB input and output throughput, DB CPU and memory usage, number of anomalies	Hierarchical Temporal Memory	Real time analysis of wearable sensor data streams
Pace et al. (2018)	Framework, implementation	Heart rate traces	Reduce the data traffic towards Internet	Transmitted traffic and processing time	NA	Heart rate monitoring to execute life critical service
Queralta et al. (2019)	Framework, implementation	MobiAct	Increase IoT device battery life, waive the need for sending raw data to cloud servers	Classification accuracy	LSTM RNN	Health monitoring
Hu et al. (2019)	Framework	Physiological	Minimize response delay	Disease's classification accuracy, response delay	Cascaded deep learning	Alarm system using chronic disease prediction
Kharel et al. (2019)	Architecture, implementation	Heart rate data	Minimize burden on the cloud, save energy	SNR, Path loss (dB)	NA	Healthcare remote monitoring

Reference	**Contribution category**	**Data type or data set**	**Main Objective of exploiting edge computing in healthcare IoT**	**Performance metric**	**ML-based approach**	**Use case**
Wu et al. (2019)	Implementation	Environmental, physiological	Process the raw sensor signals, monitoring the environmental and physiological data, trigger alert	NA	NA	Saftey and health monitoring
Uddin (2019)	Activity classification	Multiple healthcare sensors	Reduce healthcare cost, fast computation of experimental data	Classification accuracy	Recurrent neural network	Activity classification
Azimi et al. (2019)	Abnormaly detection and classification	Arrhythmia	Improve the availability, reduce response time	Classification accuracy, execution time, response time, transmission time	CNN	Detect and classify different abnormalities in ECG signals
Ram et al. (2019)	Activity classification	Physionet	Reduce large computing and communication overhead	Classification accuracy	SVM and random forest	Mobile health monitoring of human activity
Devarajan et al. (2019)	Risk-level diabetes prediction	UCI PAMAP2	Improve the bandwidth efficiency, energy, prediction accuracy, computational complexity and latency	Classification accuracy	J48 decision tree	Real time monitoring the blood glucose level

Reference	Contribution category	Data type or data set	Main Objective of exploiting edge computing in healthcare IoT	Performance metric	ML-based approach	Use case
Hayajneh et al. (2019)	Data protocol	Simulated	Channel assignment: avoid interference. Gateway association: improve the efficiency and security. Routing protocol: minimize delay and power at nodes	PDR, Delay	NA	Secure and efficient data delivery
Abdellatif et al. (2020)	Framework, implementation	Multimodal	Compress data, extract feature and detect seizure by deep learning based classification to boost the system performance, reduce the transferred data, preserve data privacy	Distortion ratio, battery level, classification accuracy	Deep learning, unsupervised learning, reinforcement learning	Realtime patient remote monitoring
Hegde et al. (2020)	Disease detection	Thermal video, visible light	Rapid response, separate interaction between patients and healthcare worker	Classification accuracy	Deep learning	Assist in the automatic triage of patients in emergency department
Abdel-Basset et al. (2020)	Type 2 diabete detection	Various biological	Improve response time and privacy	Execution time accuracy	Neutrosophic	Detecting and monitoring patients with type-2 diabetes

Table 1.4. *Edge computing in healthcare IoT*

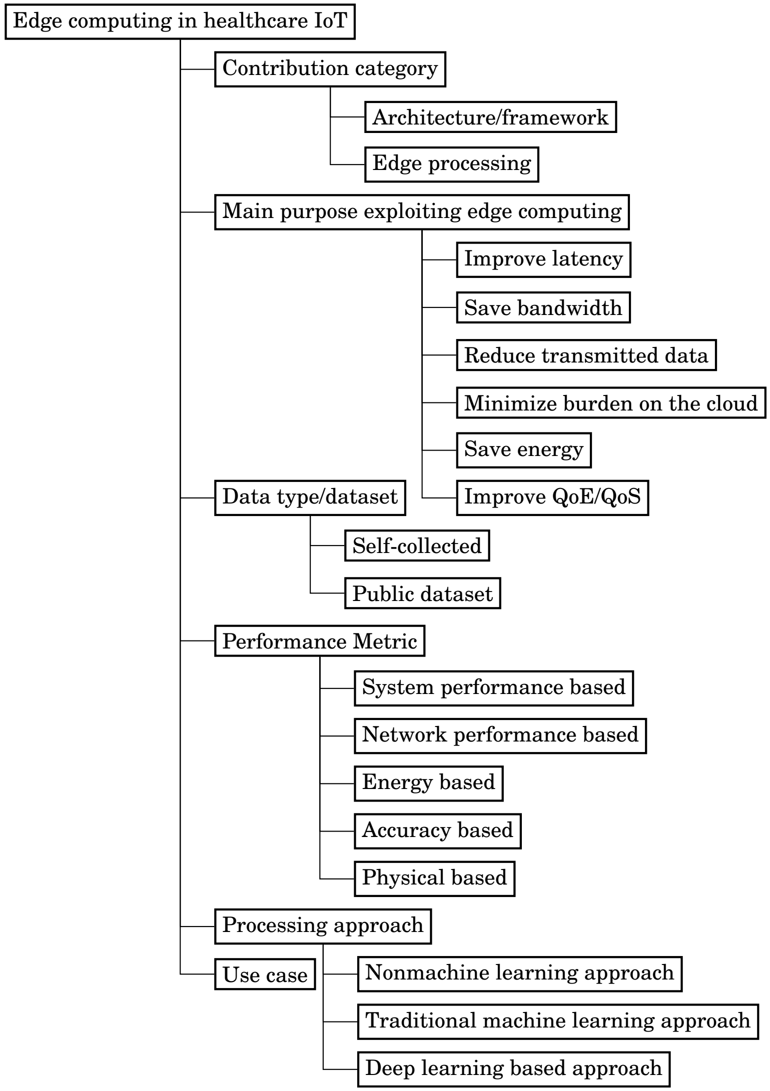

Figure 1.4. *Edge computing's taxonomy in Health-IoT*

The main reason for such challenges is the Internet's expansion on both horizontal and vertical scales to meet human demands. Besides, the heterogeneity and fragmentation in the field caused by the diversity of Internet software solutions and hardware equipment that have not been resolved effectively also escalate the situation. Not to mention, the compatibility of the existing infrastructure to the novel advancements in the field is also challenged by these complications. To handle such sophisticated state of the Internet, it is required the most resourceful organizations to manage the worldwide digital space. In this case, the companies (ISPs, MNOs, etc.) are the only feasible candidates. From end-user expectations, the Internet operation is supposed to be stable and work flawlessly. Hence, any disruption in Internet services could cause tremendous consequences to the companies' operations and revenues (Siddiqui 2021). A considerable expense will be saved if the operator can foresee and manage unfavorable events before their occurrences.

To deal with such uncertainty and complexity, a novel solution is introduced and adopted by the community, that is, software-defined network (Bannour et al. 2018). By decoupling the control plane and data plane, SDN provides a top-down network view, which is crucially vital in Internet management operations. Thus, the research community has proposed and adopted various SDN applications in the literature over the years. Sharing the equivalent expansion and diversity with the Internet, IoT is the next promising land for software-defined network's management capability. The paradigm's potential in the H-IoT domain remains to be explored. In the subsequent discussion, we uncover the SDN landscape in the H-IoT literature.

1.2.2.2. *Software-defined network's taxonomy in H-IoT*

Utilizing the same approach to the edge computing paradigm, we initiate the SDN's SOTA in H-IoT with architectural contributions.

Sinh et al. (2018) is one of the first works laying the foundation for this research direction. The authors addressed the role of SDN in IoT deployment, which is orchestrating the whole network. They also introduced an SDN-based architecture for IoT deployment.

Meanwhile, Baktir et al. (2018) presented a multi-tier computing and communication architecture for pervasive healthcare (including IoT) powered by SDN. The work aimed to investigate SDN's capability to handle the personalization of healthcare services and the delay sensitivity of continuous health assessment while exploiting the edge computing potential to deal with latency-intolerant services.

In addition to the SDN management enhancement to the H-IoT system, SDN also solidifies H-IoT infrastructure by enhancing its security. El Jaouhari and Bouabdallah (2018) studied the security mechanism including the confidentiality, integrity, authentication and access control of the H-IoT system. The current work was limited to the security management of a single infrastructure. However, the authors claimed to extend the extension in their future work. Nevertheless, the results indicated the necessity to improve the single-point controller performance to cope with the H-IoT security issues effectively. Taking the SDN bottleneck drawback into consideration while securing the H-IoT system, Aujla et al. (2019) proposed to move SDN from a cloud environment to an edge–cloud environment. The authors offered three main contributions to this work. First, they presented an offloading scheme aimed to support edge-cloud interactions. Their flow management scheme aimed to achieve the optimal flow path, reducing network delay even the number of healthcare devices and end-to-end distance increases. Finally, they also improve the system's security with a lattice-based cryptosystem. Taking a step further, Li et al. (2020) also adopted the edge-computing paradigm but for load balancing purposes. They also proposed a lightweight authentication scheme to enhance system security.

Besides proposing architectures that aim to improve security and centralized bottleneck aspects, other researchers also investigated various architectures to enhance general network performance in SDN-enabled H-IoT systems. In 2019, Cicioğlu and Çalhan (2019a) and Cicioğlu and Çalhan (2019b) presented their work about their SDN-based architecture and a novel energy-aware routing algorithm. The results confirmed their SDN-based structure meets the expected QoS and the routing approach is superior to the traditional routing approach in terms of energy consumption, throughput, successful transmission rate and delay. Afterward, Preveze et al. (2022) also studied the subject but focus their work on developing a novel adaptive switching technique. Via MATLAB simulation, they succeeded in increasing the throughput performance and promised to develop further the proposed system considering the energy factor.

Using SDN's orchestrating capability, Hasan et al. (2020b) proposed an SDWBAN framework to prioritize sensitive healthcare data over ordinary data. They employed an application classification algorithm and a modified sector-based distance (SBD) protocol version to implement data prioritization. Later, the authors developed a mathematical model to determine the optimal number of controllers for the proposed framework in Hasan et al. (2020a). The results show the latency and PDR performance improvement, which ensures the efficiency of their proposed SDN's administrative data scheme. Furthermore, Lakhan et al. (2022) also investigated this research direction but focused on a different aspect, the resource allocation problem. They modeled the SDN-enabled H-IoT system as a geographically distributed fog network, later formulating a multi-constraint optimization problem. A deep-learning Q-network-based resource allocation scheme was presented based on the prepared architecture and later proved its performance improvement. Misra et al. (2023) approached this research direction by offering on-the-fly analytics to the end devices. The SDN administration tasks in this work, such as reconfiguration and programmability, were considered at three stages: resource based, flow rule based, and analytics based. A large-scale simulation evaluation using Mininet highlighted the architecture efficiency by eliminating additional network delay. In the meantime, Sarkar et al. (2023) approached the problem under the server selection scope. They provided a framework taking advantage of game theory's approach to transfer information to the fog/cloud layer. In this work, they also utilized a three-layered CNN to detect patient's communicable illnesses. Jameel et al. (2020) also took advantage of SDN's orchestrating capability but focused on physical signal performance. The authors proposed a Q-learning-based optimization framework for mitigating the impact of interference in SDN-based backscatter heterogeneous networks. Their simulation results showed the increase in performance of the macro-cell users while maintaining a favorable SINR's level for backscatter users in the small cell.

Besides architectural contributions, various works concentrated on other specialized topics in SDN H-IoT-based systems. In the security aspect, in 2018, Meng et al. (2018) paved the way by introducing a Bayesian-based trust model for detecting malicious devices in SDN-based H-IoT. Their results demonstrated that the trust values of malicious devices using their proposed approach decreased faster than the SOTA, thus improving the identification stage. Later, in 2022, Radoglou-Grammatikis et al. (2022) presented a study about the IEC 60 870-5-104 protocol. Assessing this protocol, the authors provided a quantitative threat model that relied on attack defense trees and common vulnerability scoring system. They also presented an intrusion detection and prevention system derived from the proposed threat model. Various machine learning and deep learning techniques have been utilized to ensure their system's performance. Later, in 2023, Halman and Alenazi (2023) and Alzahrani and

Alenazi (2023) also focused on this direction and succeeded in increasing the SOTA successful detection rate impressively to more than 99%. In network performance, Misra et al. (2020) proposed a hybrid flow-rule replacement scheme that dynamically places or removes flow rules at the edge access point. The proposed method also considered users' criticality and mobility in healthcare scenarios. The achieved result confirmed significant latency, overhead and energy consumption reduction. From a scheduling perspective, Askari et al. (2021) proposed a two-tier mechanism for scheduling transmission from hubs to the APs. The proposed algorithm considered channel conditions, energy consumption and the highest priority to reduce the average delay and energy consumption and increase the effective throughput.

After the brief introduction to SDN's state of the art in H-IoT, we generalize research topics in the domain in Figure 1.5 and highlight chapter's content in Table 1.5.

1.3. Learned lessons and neglected opportunities

1.3.1. *Learned lessons*

Considering the presented state of the art, we structure our best understandings about explored topics of SDN and MEC in the H-IoT domain by Figure 1.6. From our point of view, we outline three major learned lessons from the literature's current state as follows.

First, the H-IoT system is usually formulated using the three-layer architecture: the Things, Processing and Communication layers. However, most researchers have been focusing on the processing tasks at the Things or Processing layers. Their investigations are the backbone for enabling future feasibility in this field.

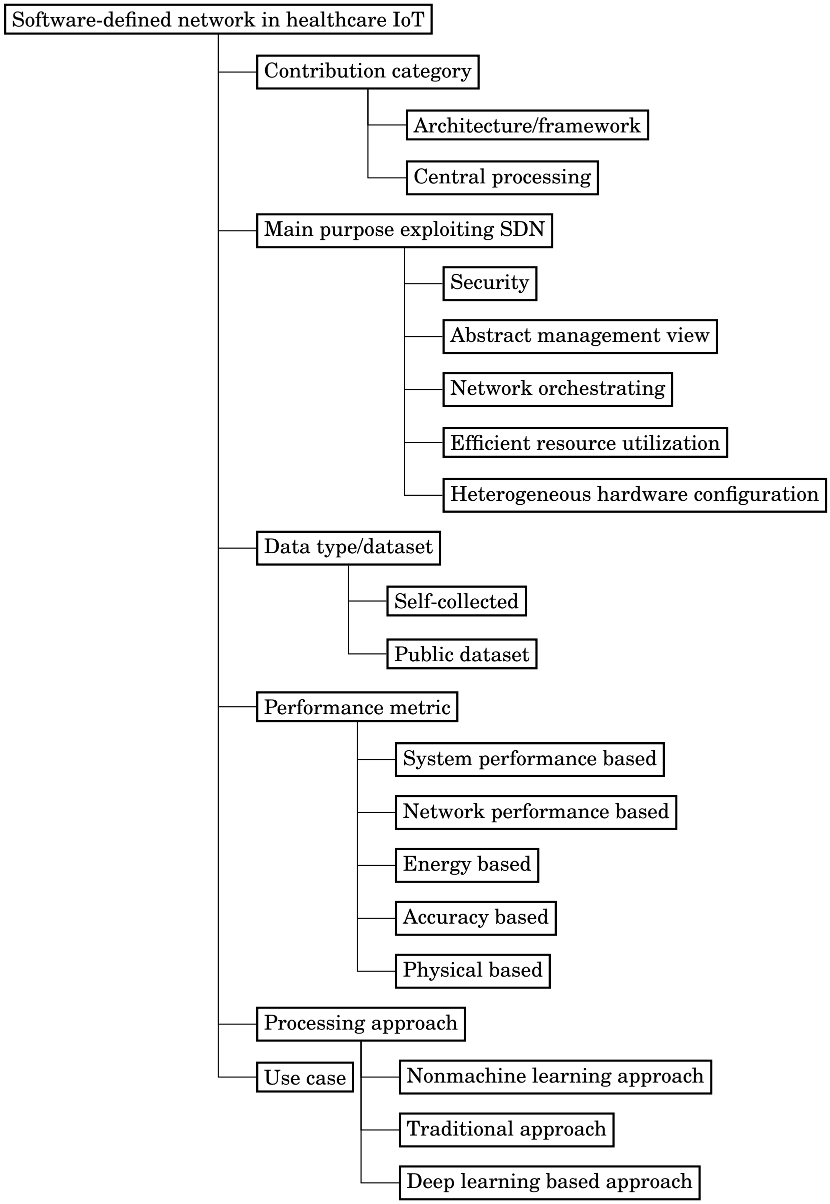

Figure 1.5. *Software-defined taxonomy in Health-IoT*

Reference	**Contribution category**	**Data type or data set**	**Main Objective of exploiting software-defined networking in healthcare IoT**	**Performance metric**	**ML-based approach**	**Use case**
El Jaouhari and Bouabdallah (2018)	Architecture	ZAP-based synthesized data	Solve securities issues (confidentiality, integrity, authentication, access control) in a smart infrastructure	RTT, CPU usage, request analysis, switch's network IO	Nonmachine learning	System security and monitoring
Sinh et al. (2018)	Architecture implementation	NA	Network orchestrating to build on-demand IoT service via network slicing	Service testing	Nonmachine learning	Network orchestrating
Meng et al. (2018)	Security model	Self-synthesized	Quick response to handle the identification in the insider attacks.	Trust value, CPU usage	Bayesian model	Intrusion detection
Baktir et al. (2018)	Architecture, fall risk assessment	Self - synthesized	Efficient manage the resource allocations and facilitate personalized healthcare services	Service delay, CPU usage, classification accuracy, decision boundary	SVM and random forest	Fall risk assessment
Aujla et al. (2019)	Framework	Self-synthesized	Real-time analysis with seamless and secure transmission, ensure Quality of Service	Offloading rate, latency, complexity, network delay, number of handover	Nonmachine learning	QoS assurance

Reference	**Contribution category**	**Data type or data set**	**Main Objective of exploiting software-defined networking in healthcare IoT**	**Performance metric**	**ML-based approach**	**Use case**
Cicioğlu and Çalhan (2019b)	Routing algorithm	Self-synthesized	Centralized control to integrate and manage network infrastructures through a standard interface	Throughput, successful transmission rate, end-to-end delay, energy consumption	Nonmachine learning	Inter-WBAN communication
Cicioğlu and Çalhan (2019a)	Architecture, Interface protocol	Self-synthesized	Complex network infrastructure management	Throughput, delay, PDR, average energy consumption, BER	Nonmachine learning	Handling heterogeneous WBAN structures
Hasan et al. (2020b)	Framework	Simulated data (Castalia)	Provide administrative control for WBAN	PDR, CDF, latency	Nonmachine learning	Real time patient monitoring
Li et al. (2020)	Framework	Simulated data	Efficient resource utilization	Delay, throughput, control overhead, average response time, PDR	Nonmachine learning	Securing system and and effective resource utilization

Reference	Contribution category	Data type or data set	Main Objective of exploiting software-defined networking in healthcare IoT	Performance metric	ML-based approach	Use case
Hasan et al. (2020a)	Network optimization	Simulated data (Castalia)	Abstract view to manage network and efficient resource utilization	PDR, delay	Nonmachine learning	Exploring mathematical relationship
Misra et al. (2020)	Person's criticality trajectory prediction	Heart Disease UCI	Heterogenous hardware configuration, better control in traffic forwarding, channel allocation	Accuracy, latency, energy, overhead	Decision tree, Naive Bayes	Prioritize healthcare traffic
Jameel et al. (2020)	Q-learning model	Time-series heart rate data	Heterogenous hardware configuration	SINR	Reinforcement learning	Backscatter communication in healthcare
Askari et al. (2021)	Multi-access schedule algorithm	Simulated data	Abstract view to manage network and efficient resource utilization	Effective throughput, average energy consumption, average delay	Deep neural networks	Real-time healthcare monitoring

Reference	**Contribution category**	**Data type or data set**	**Main Objective of exploiting software-defined networking in healthcare IoT**	**Performance metric**	**ML-based approach**	**Use case**
Radoglou-Grammatikis et al (2022)	Quantitative threat model	Synthesized IEC 60 870-5-104 dataset	SDN's attack mitigation mechanism	Detection performance, classification accuracy, mitigation performance	Multi armed bandit, classification regresion decision tree, reinforcement learning with Thomson sampling	Secure healthcare infrastructure
Alzahrani and Alenazi (2023)	Attack detection	MCAD-SDN	Ensure efficient resource utilization, security, optimal network control and management	Detection classification accuracy	KNN, decision tree, random forest, naive bayes, logistic regresion, ada boost, extreme gradient boosting	Secure healthcare infrastructure
Preveze et al. (2022)	Adaptive switching algorithm	MATLAB simulation	Manage complex healthcare IoT networks	Throughput	Nonmachine learning	Real-time health monitoring
Lakhan et al. (2022)	Architecture, lightweight Q-model-based policies	Simulation	Handling challenged resource allocation in mobility and distributed dynamic fog networks	Resource utilization, latency, energy consumption	Deep reinforcement learning	Resource allocation

Reference	**Contribution category**	**Data type or data set**	**Main Objective of exploiting software-defined networking in healthcare IoT**	**Performance metric**	**ML-based approach**	**Use case**
Halman and Alenazi (2023)	Attack detection	MCAD-SDN	Ensure efficient resource utilization, security, optimal network control and management	Detection classification accuracy	KNN, decision tree, random forest, naive bayes, logistic regresion, ada boost, extreme gradient boosting	Secure healthcare infrastructure
Sarkar et al. (2023)	Communicable illness detection	Simulation	Reduce latency, increase total network longevity	Delay, energy consumption	CNN	Illness detection
Misra et al. (2023)	Architecture	Simulation	Identification, dynamic management of services, and fast analysis	Response time, latency, PDR, throughput	Nonmachine learning	Remote healthcare monitoring

Table 1.5. *Software-defined networking in healthcare IoT*

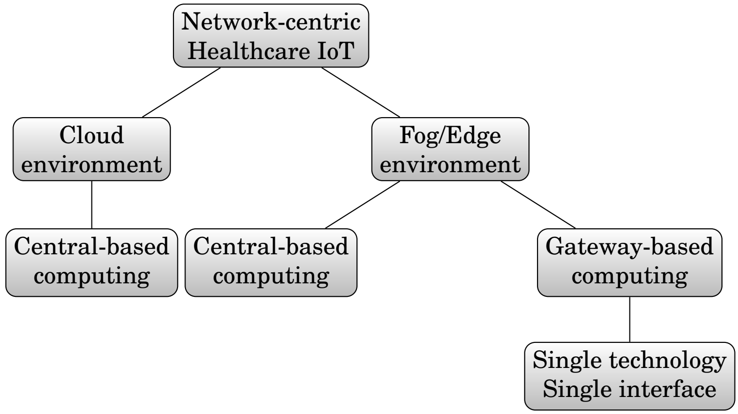

Figure 1.6. *Explored research topic generalization in network-centric healthcare IoT*

Furthermore, most research is being conducted with a few presumptions: the end user gateway and the designated central server are identified and expected to be kept unchanged. At the same time, the middleware network infrastructure is *managed by MNOs and ISPs* and *exclusively* depend on them to ensure *a stable channel*. Despite the development of various communication technologies extending both the range and bandwidth for the transmission channel, these assumptions could only be satisfied under the following conditions. Both client–server endpoints are *static and utilize an unyielding* network infrastructure for their interactions. In other words, the communication infrastructure must be stable throughout the H-IoT transmission process. However, these criteria are hard to convince as the only typical scenario in our studying domain, since one endpoint mainly is the human body, and its mobility factor requires considerate attention. Besides the end-users mobility, among various challenging factors, such as the high-density deployment of advanced middleware network infrastructure (5G and 6G) and the dynamicity in complex central computing environments, etc., the expectation about the above network conditions seems unrealistic. In addition, we have also addressed that the 5G novel concept, network slicing, has opened the opportunities to hand over the network management to the customer. Second, current H-IoT communication utilizes only *one communication interface* for transmission purposes. Nevertheless, no study or countermeasure in the domain is proposed or implemented to allow for a seamless network experience despite any unpredictable obstacle that may cause a function disruption to the only interface. Considering the operational and environmental uncertainty, especially in the context of this work, that is, healthcare emergencies, it is also challenging to guarantee the reliability of the client-side transmission in such conditions.

Lastly, the H-IoT system formulation requires numerous design decisions depending on each use case. After the system design process, the technology combinations in the three-layer architecture must be chosen. The community has offered various solutions in each subdomain in the physical and virtual layers. However, this diversity without a common standard also causes heterogeneity and fragmentation issues to develop and deploy the decided solution.

A noteworthy example of this situation is the diversity in communication technology in the Communication layer (Tables 1.2 and 1.3). Thus, these problems have been challenging academia and the industry for decades and have not been resolved effectively yet.

From the deriving knowledge, we explain our critical thinking process and the reason for our research decisions in this work in the subsequent discussion.

1.3.2. *Neglected opportunities*

Exploiting the network landscape preview and our learned lesson about the SOTA of SDN and MEC paradigm in the H-IoT domain, we list the neglected opportunities awaiting to be discovered by the community as follows:

– The opportunity to manage the network infrastructure has yet to receive its deserved attention from the eHealth researchers despite its promising impact.

– Since most of the research is based on stable network and infrastructure conditions, more foundation investigations should be conducted toward flexible and dynamic network infrastructure in the H-IoT domain. The usage of multi-technology and multi-radio utilization and their potential in the domain have yet to be fully explored, despite being briefly mentioned in some work. A unified solution to the domain's heterogeneity and fragmentation issues has yet to be proposed in the literature.

Considering all of the insights above and the criticality of delivering vital healthcare data in real-time in H-IoT urgent situations, we recognize the missing gap between stable and static and flexible and dynamic network infrastructure in the H-IoT domain. Besides, the open challenges in dealing with heterogeneity and fragmentation in the literature are awaiting to be resolved. These facts motivate our research toward providing the unveiling solutions for the H-IoT domain in such directions. While proposing solutions for the heterogeneity and fragmentation issues in the H-IoT domain, we also harness the undiscovered prospect of utilizing multiple communication interfaces simultaneously for the best network performance and cutting-edge transport protocols to maintain a seamless network experience for the terminal node, especially in the 5G era's context. Despite focusing on the most challenging and uncertain network conditions in the H-IoT branch, our research prospects are unlimited and applicable to the general IoT context or other domains. Figure 1.7 depicts the book's research directions and our contributions' positions in the innovated literature.

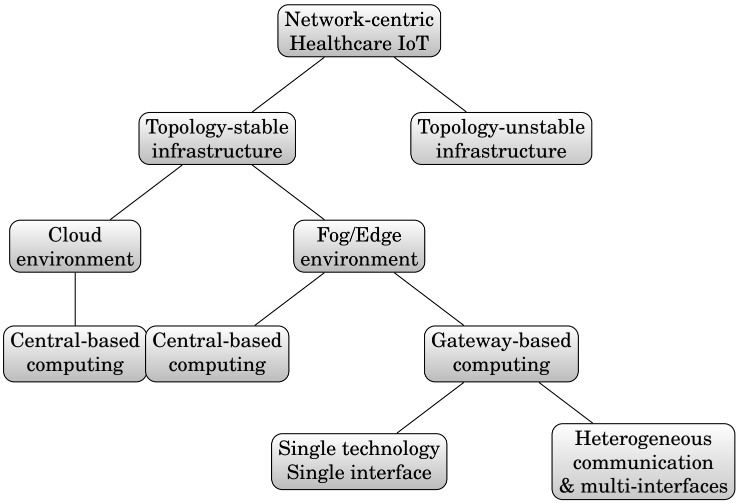

Figure 1.7. *Proposed research directions in network-centric healthcare IoT. For a color version of this figure, see www.iste.co.uk/chu/softwaredefined.zip*

1.4. Conclusion

This chapter has presented an overview of the H-IoT domain and its key enablers. We also create taxonomies from the studied work, which later help us extract the learned lessons and neglected opportunities in the domain. From the extracted insights, we navigate our research to focus on the undiscovered directions that take healthcare emergencies into prioritized consideration. However, thanks to their genericity, the prospect of the proposed solutions is applicable to the general IoT context or other domains. The following chapters will describe our proposed solutions and their prospective impacts in more detail. The next chapter presents our first contribution of software-defined network, a novel network paradigm.