Reliable and Resilient AI and IoT-Based Personalised Healthcare Services: A Survey

NAJMA TAIMOOR AND **SEMEEN REHMAN**
Institute of Computer Technology, Technische Universität Wien (TU Wien), 1040 Wien, Austria
Corresponding author: Najma Taimoor (e1155891@student.tuwien.ac.at)

ABSTRACT Recent technological (e.g., IoT, 5G), and economic (e.g., UN 2030 Sustainable Development Goals) developments have transformed the healthcare sector towards more personalized and IoT-based healthcare services. These services are realized through control and monitoring applications that are typically developed using artificial intelligence (AI)/machine learning (ML) based algorithms, that play a significant role to highlight the efficiency of traditional healthcare systems. Current personalized healthcare services are dedicated in a specific environment to support technological personalization (e.g., personalized gadgets/devices). However, they are unable to consider different inter-related health conditions, leading to inappropriate diagnosis and affect sustainability and the long-term health/life of patients. Towards this problem, the state-of-the-art Healthcare 5.0 technology has evolved that supersede previous healthcare technologies. The goal of healthcare 5.0 is to achieve a fully autonomous healthcare service, that takes into account the interdependent effect of different health conditions of a patient. This paper conducts a comprehensive survey on personalized healthcare services. In particular, we first present an overview of key requirements of comprehensive personalized healthcare services (CPHS) in modern healthcare Internet of Things (HIoT), including the definition of personalization and an example use case scenario as a representative for modern HIoT. Second, we explored a fundamental three-layer architecture for IoT-based healthcare systems using both AI and non-AI-based approaches, considering key requirements for CPHS followed by their strengths and weaknesses in the frame of personalized healthcare services. Third, we highlighted different security threats against each layer of IoT architecture along with the possible AI and non-AI-based solutions. Finally, we propose a methodology to develop reliable, resilient, and personalized healthcare services that address the identified weaknesses of existing approaches.

INDEX TERMS Healthcare 5.0, IoT, medicine 4.0, reliability, resilience, personalization, sustainability.

I. INTRODUCTION

Contemporary social and economic developments around the globe e.g., UN Sustainable Agenda 2030 [1], are aiming to extend life expectancy for all humans by improving their physical and mental health, and well-being. Current technological advancements have helped to achieve this agenda in real-time. To this end, various dedicated technical initiatives have been introduced, for instance, one such initiative is ''Healthcare 5.0'' which has been developed as a result of the emergence of digital wellness and a new digital standard for healthcare services [2]. Furthermore, recent development in technology has enabled remote and automatic monitoring of healthcare services through medical

The associate editor coordinating the review of this manuscript and approving it for publication was M. Shamim Hossain.

devices that aims to monitor various health conditions of a patient. Importantly, these devices are dedicated to specific health conditions and work independently. For instance, blood pressure monitor aims to monitor only heart-related health conditions, insulin pump only regulates diabetic health conditions through maintaining the right level of blood insulin, to name a few.

Prior to Healthcare 5.0, ''Healthcare 4.0'' had emerged from Industry 4.0, that had transformed the healthcare sector into more digital during the past decade. For instance, x-rays and magnetic resonance imaging (MRI) have transformed into computer tomography (CT) and ultrasound scans to electric medical records [3]. These devices are user-centric that are used by caretakers/ medical practitioners to monitor and treat medical conditions of patients, in preventive care, and for well-being solutions. With the recent advent

FIGURE 1. Economic impact of IoT devices and applications.

FIGURE 2. Reliability.

of technologies (e.g., Industrial Internet of Things IIoT, Industrial cyber-physical systems ICPS), the use of IoT devices and applications is exponentially growing. According to [4] by the end of 2021, the IoT devices and applications are expected to reach 212 billion, whose major use is in healthcare (~ 41%) as shown in Figure 1. Furthermore, as reported by Grand View Research [5], the healthcare IoT market is expected to be worth USD 534.3 billion by 2025.

The principle goal of technology-driven applications in healthcare is to support healthcare operations by automatically controlling various health conditions of patients through continuous and remote monitoring of the conditions [6]–[8]. Following the principle, Healthcare 5.0 aims to support various objectives, i.e., (i) reliable, (ii) resilient, and (iii) personalized healthcare services in real-time. In the following, we discuss our taxonomy that characterizes the aforementioned healthcare objectives.

- **Reliability:** Analogous to the definition of reliability by IEEE Standards [9], we consider the reliability of healthcare services as the ability of the services to perform their required functions consistent with stated conditions (aka specification) for a specified time as shown in Figure 2. Healthcare 5.0 supports automatic monitoring and control of underlying health conditions of patients. Therefore, these services must be extremely reliable (i.e., they must perform required operations as expected under normal and stated conditions). Otherwise, the services may fail to operate as expected leading to severe consequences, including threatening the lives of patients. To establish reliability, various efforts [10]–[12] have identified different factors (e.g., battery, memory, computational power, enhancement of QoS) that can improve the reliability of the healthcare services by using modern solutions e.g., blockchain-based technologies.

- **Resilience:** We adapt the definition of resilience from different interpretations [13], [14], as the ability of healthcare service to continue its required function in the face of adverse operating conditions. To this end, a resilient service first detects an adverse condition (e.g.,
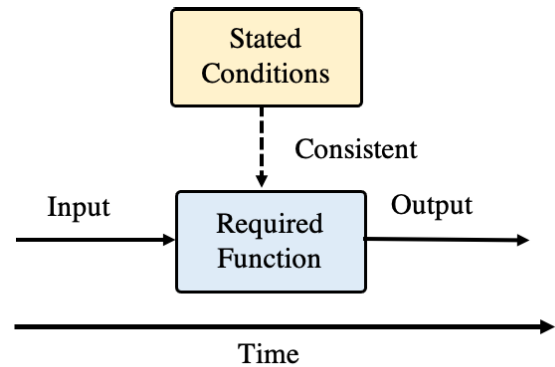
fault, error, bug, and cyber threat) that malfunctions it, then recovers the required function of the service by mitigating the impact of the adverse condition as shown in Figure 4. Healthcare 5.0 services need to be resilient to support continuous monitoring of health conditions, i.e., to continuously deliver correct functionality and availability of the services to the user despite adverse environmental conditions, internal faults of the system such as hardware and software defects, cybersecurity threats, and vulnerabilities, excessive loads, age, and wear, and degraded communications [13]. Any disruption of the services due to intentional or accidental incidents may also threaten patients' lives. To establish resilience, various efforts [15], [16] have recognized potentially vulnerable functions (e.g., failure of software, hardware, cloud services, and communication devices) that may hinder the resilience of healthcare attributes and proposed different ways to recover from them (e.g., post-event automatic recovery of the vulnerabilities like Moving Target Defense (MTD) [17], and blockchain-based solutions [18]).

- **Personalization:** Personalized healthcare services typically operate in the most strict mode by supporting customization of a specific health condition under specific conditions [19], [20]. This does not work in practice because patients with long-term health conditions often have multiple health conditions. Therefore, we realize personalization of healthcare service as the ability of the service that provides determinant-based (e.g., genetics, behavior, environmental and physical influences, medical care, and social factors) optimization of multiple health conditions of a patient as shown in figure 3. The optimization extends the life expectancy of the patient by reducing the side effects of various health conditions.

Based on our taxonomy, we extend Healthcare 5.0 to support personalized healthcare services that aim to optimize clinically inter-related multiple health conditions of a patient. As sketched in Table 1, the current infrastructure (i.e., software and hardware) of healthcare services supports complementary technological and clinical personalization. Former approaches

TABLE 1. Perspective-based healthcare system/infrastructure components.

| Components / Perspective	Hardware	Software
Technological	Personalized medical devices and gadgets (e.g., Smart shirts and watches)	Technology-driven applications (e.g., AI/ML-based patient specific control and monitoring applications)
Clinical	Underlying sensing infrastructure (e.g., Bio and pressure sensors)	Clinical process-driven applications (e.g., AI/ML-based diagnosis and treatment applications)
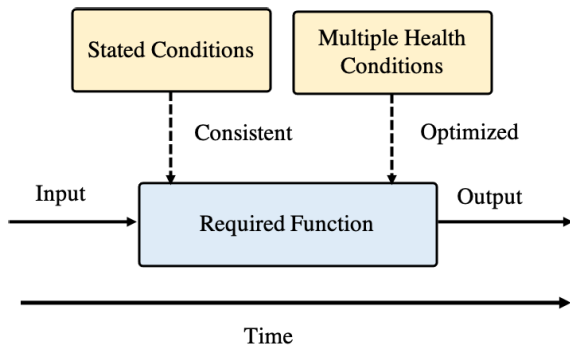
FIGURE 3. Personalization.

aim to develop personalized medical gadgets (e.g., customized hearing aid, artificial placenta [21], wearable insoles [22]) and applications (e.g., Basal and bolus insulin settings in insulin-pump [23], fitbit+ [24]) for handling specific technical needs of a particular health condition. Latter approaches aim to develop personalized medical technologies (e.g., enzyme-based biosensors for sweat analysis [25], antibody-based sensor for rapid detection of avian coronavirus [26]) and applications (e.g., ML-based algorithms [27], clinical-parameter -based configuration of insulin-pump [28]) for handling specific biological effects of a particular health condition.

As discussed above, current approaches to establish reliability, resilience, and personalization of healthcare services fail to support continuous monitoring of health conditions in Healthcare 5.0 mainly because they are either health condition-specific, or environment-specific, or agent-specific. Moreover, the emergence of new IoT medical devices manufactured by different vendors and their communication through different protocols have made the task of establishing the above-mentioned requirements more challenging. Therefore, in this survey, we systematically study and analyze various approaches that establish key requirements of the services and identify gaps that help to establish Healthcare 5.0 services in practice.

Our Contributions: To the best of our knowledge, this is the first attempt that identifies and studies key requirements

of HIoT to support clinical personalization of healthcare services (we call it CPHS) in contrast to the existing ones that support only technological personalization. We summarize our contributions as follows:

1) We defined novel comprehensive personalized healthcare services (CPHS) by contextualizing HIoT (Healthcare 5.0) to support clinical personalization
2) We identified key functional (reliability, resilience, and personalization) and non-functional (constraints on reliability, resilience, and personalization) requirements of the CPHS
3) We introduced an example use case scenario as a representative for modern HIoT
4) We explored and analyzed (strengths vs weaknesses) various AI and non-AI-based approaches to establish the identified requirements of HIoT (e.g., reliability, resilience, and personalization) in each layer of the reference architecture (i.e., things, communication, and application layer) under normal and hostile conditions (e.g., security threats).
5) Finally, we discussed our proposed methodology to provide state-of-the-art reliable, resilient, and real-time comprehensive personalized healthcare services that address the identified weaknesses of the existing approaches.

The overall logical organization of the paper is sketched in Figure 6. The rest of the paper is organized as follows. Section II explains our survey methodology. Section III introduces the transformation of healthcare technology, personalized healthcare, and their key operational requirements along with the example use case scenario. Section IV gives an overview of a reference architecture for IoT-based healthcare systems, their different layers, and recent efforts to establish requirements of the modern personalized healthcare services. Section VI provides an overview of security threats at IoT layers and types of attacks on each layer, while Section VII introduces our proposed solution. Finally, Section VIII concludes our paper.

II. SURVEY METHODOLOGY

We have performed a survey in a very systematic way by identifying top research findings in the domain of IoT and healthcare. We extracted information and summarised
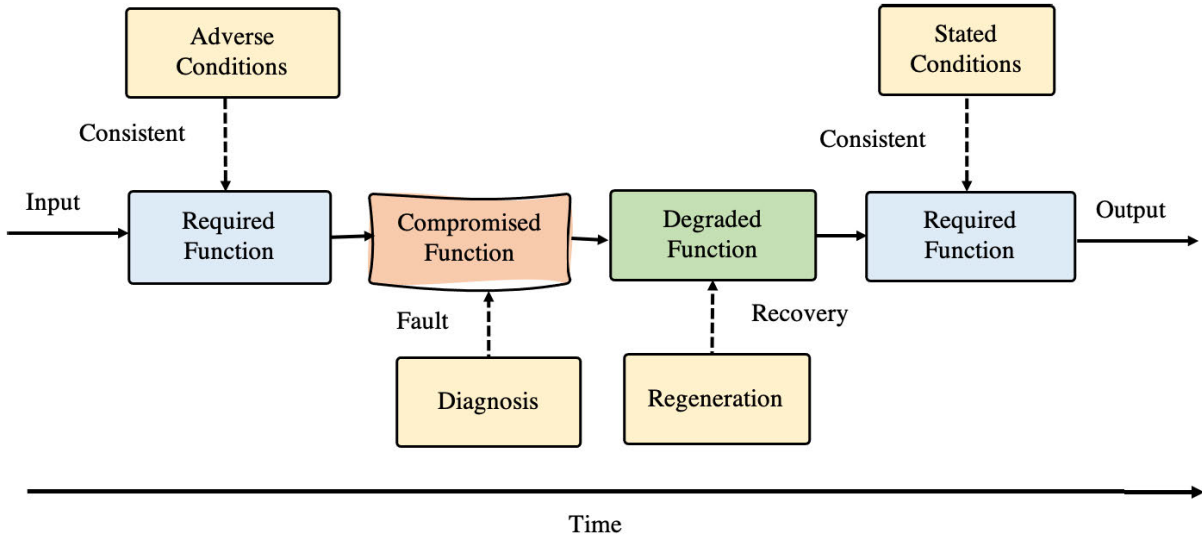
FIGURE 4. Resilience.

the current literature according to the guidelines suggested by Kitchenham [29], [30]. Our approach follows a defined sequence of steps using a systematic literature review (SLR) [31], started from downloading related research articles, reports, and thesis using keyword-based query-searching mentioned in Table 2. Our initial web search found more than 30000 papers from different data sources, e.g., Springer, IEEE, Science Direct, Academic medicine, ACM. Papers were accessed mainly from google scholar. Then our refined search based on related keywords (e.g., healthcare systems, IoT, healthcare 5.0, medicine 4.0, personalized healthcare) found approx. 200 papers. Our final refinement eliminated further 40 papers that were highly theoretical and from non-scientific sources. The remaining papers also included surveys in healthcare, however, most of these surveys [32]–[34] are focused on monitoring specific health conditions (e.g., cardiovascular, breathing problems, diabetes, etc.) in a specific environment [35], [36] (e.g., smart home, assisted living environment, elderly homes,) for specific healthcare services (e.g., wellness services and health status) [37], [38] and for specific agents (e.g., caretakers, doctors) using modern infrastructure (e.g., IoT devices, 5G network, and electronic healthcare).

III. TRANSFORMATION OF HEALTHCARE TECHNOLOGY

The history of healthcare systems is deeply connected with the history of medicine. As shown in Figure 5 medicine's history starts with Medicine 1.0, where it was dependent on highly qualified doctors, and most of the medication was based on natural substances like herbs. These were the days of Healthcare 1.0, where intelligent public health approaches are used to solve significant health problems [39]. The discovery of antibiotics and the use of X-rays for diagnostic purposes has introduced the concept of big hospitals and specialization

TABLE 2. Keywords.

Healthcare	AND	
		personalization
		IoT **OR** HIoT
		Security **OR** Reliability
		Reliability **AND** Things **OR** sensors
		Reliability **AND** Things **OR** AI/ML
		Reliability **AND** communication **OR** network
		Reliability **AND** application **OR** software
		(Resilience **AND** Things) **AND** sensors
		(Resilience **AND** communication **OR** network
		(Resilience **AND** communication **OR** AI/ML
		(Resilience **AND** application **OR** software
		(security **OR** privacy) **AND** threats
		Personalization **AND** Things **OR** sensors
		Personalization **AND** communication **OR** network
		Personalization **AND** application **OR** software
		"IoT layers" **OR** "manufacturing industry"
		sensors **AND** reliability
		sensors **OR** sensor types **AND** healthcare
		Healthcare 5.0 **OR** Medicine 4.0 **AND** healthcare
		Healthcare 5.0 **OR** AI/ML **AND** Personalized healthcare
		wearables **AND** healthcare

in diagnostic techniques and is given the name Healthcare 2.0. Healthcare 2.0 was the era of industrialization and its primary structure was mass production (aka Medicine 2.0). Later surgery was benefited a lot with the new advancements in electronics and micro-technology. Evidence-based medicine, the introduction of surgical robots, navigation surgery, and image recognition had given birth to Medicine 3.0 and was the basis for Healthcare 3.0. With the advancements in information systems and technologies, intelligent devices with smart microelectronics, fast transmission and network technologies are working together in healthcare systems and are playing a significant role towards the better quality lifestyle and improved healthcare services which
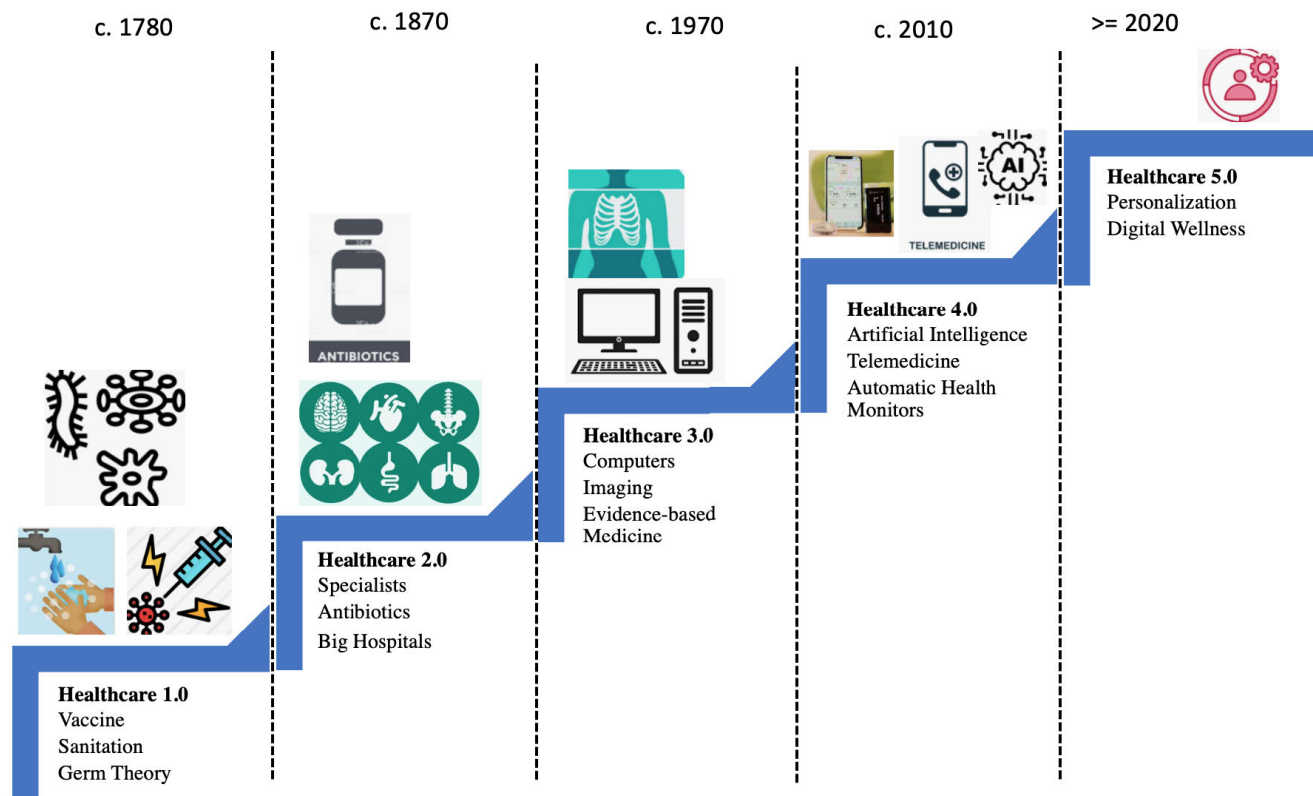
FIGURE 5. Timeline of Healthcare evolution.

TABLE 3. Developments of Healthcare (aka Medicine) 1.0 - 5.0.

| Healthcare	Developments	Era	Focus (Medicine/Healthcare)
1.0	Natural substances (herbs) Sanitation, germ theory, vaccination	Production	Public health/ Evidence-based treatment
2.0	Antibiotics, X-rays Big hospitals, professionalism, specialists	Industrialising	Mass production/Value chain
3.0	Image recognition, evidence-based, microtechnology Computer imaging and evidence-based	Automation	Information technology/Operating model
4.0	Communication + Microtechnologies Artificial intelligence, precision, telemedicine	Digitalisation	Smart health/Business model
5.0	Connectedness + Integrity Customer models, lifelong partnership, digital wellness	Personalization	Personalized medicine/Customer model

ultimately lead towards a healthier life, which is called Medicine 4.0 (aka smart-health). Some of the examples of Medicine 4.0 are personalized chemotherapy, personalized telematic therapy, intelligent implants for cancer therapy, and intelligent occlusal splint [40]. The focus of Healthcare 4.0 was to develop business models for healthcare systems. Smart wearables with integrated sensors help to collect, monitor, and diagnose diseases from the patient's data using artificial intelligence (AI)/machine learning (ML) techniques. However, IoT devices with artificial intelligence cannot be considered as a solution to the limitations (scalability, security, privacy, and reliability) in fourth-generation healthcare systems due to the following major challenges at the communication layer,

- seamless data transmission rate with minimum or no data loss,
- traffic-free transmission channels,
- cost-effective,
- no time data retrieval and
- machine to machine (M2M) or device to device (D2D) communication.

The emergence of advanced communication technologies like 5G has resolved the major challenges at the communication layer that resulted in connectedness and integration, and is the start of Medicine 5.0 (aka Healthcare 5.0). The main focus of Healthcare 5.0 is personalization by developing customer models, digital wellness, and considering the well-being of not only patients but individuals. The developments

**Reliable Resilient and Personalized Healthcare 5.0**
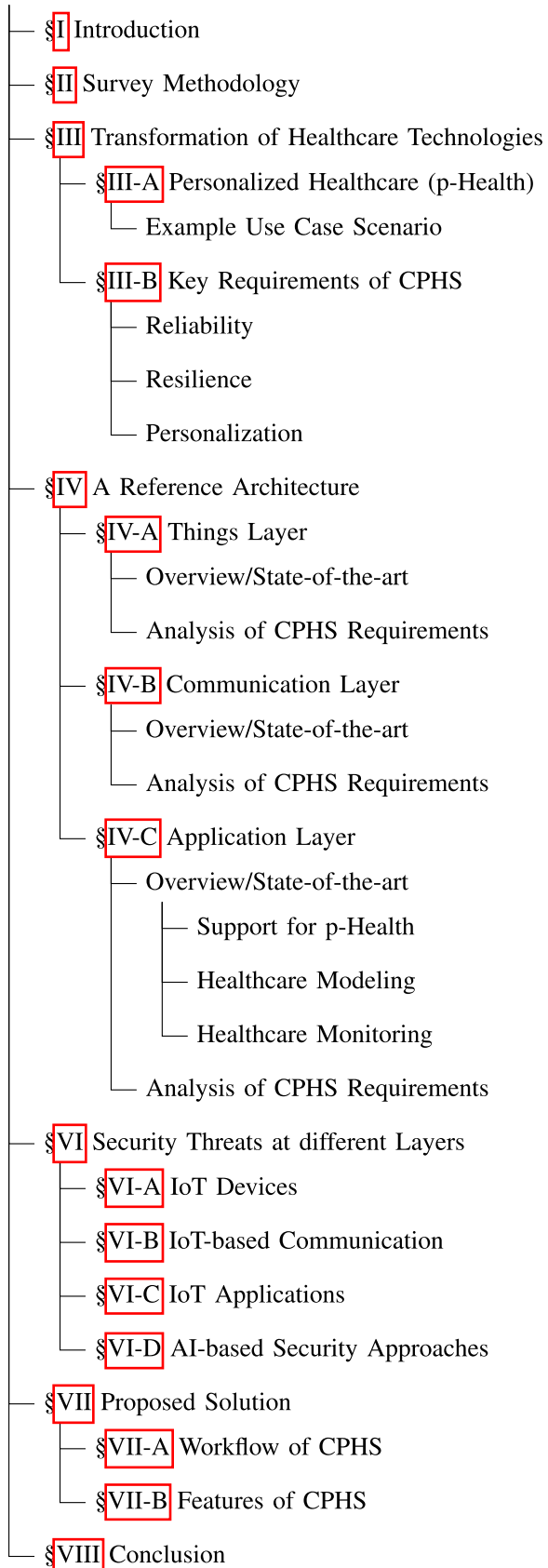
FIGURE 6. Logical structure of the paper organization.

of healthcare/medicine 1.0 - 5.0 are shown in Table 3. Other similar initiatives around the globe are Industrie 4.0 (Germany and EU), Cyber-physical systems (CPS), Society 5.0 (Japan), and Cyber social systems [40].

Based on the introduction to Healthcare 5.0, in the following subsection, we define personalized healthcare.

A. PERSONALIZED HEALTHCARE

According to the World Health Organisation (WHO), healthcare is defined as the maintenance or improvement of a complete state of physical, mental, and social well-being whose main purpose is to enhance the quality of life and to extend the life expectancy of patients. This can be achieved by enhancing their personalized health conditions.
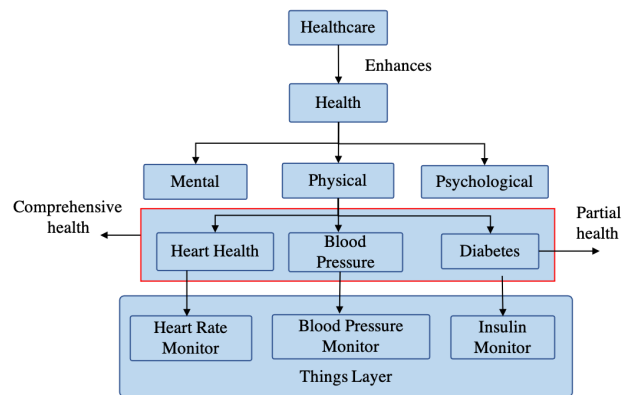
FIGURE 7. Partial vs comprehensive health.

Current approaches consider personalized healthcare as a service that tailors medical treatment to individual patients through the identification of common features, including their genetics, inheritance, and lifestyle [19]. However, this consideration helps to personalize a single health condition with specific causes (e.g., genetics, inheritance) but is unable to personalize the overall health of a patient with multiple health conditions which requires an understanding of the biological relationship among different health conditions. Furthermore, particularities of personalized healthcare are different for different patients as everyone has different health condition determinants, namely, biological, physiological, and psychological characteristics (e.g., immunity, sensitivity against variable phenomena) that play a vital role in maintaining someone's personalized health, which implies that patient's health condition parameters will also be unique.

To this end, we view personalized healthcare as a service that provides determinant-based optimization of multiple health conditions of a patient (which we call comprehensive healthcare service - CPHS). Determinant-based optimization aims to improve the long-term overall health of a patient by reducing side-effects of different health conditions of the patient (e.g., heart condition, blood pressure condition, insulin condition), while considering the relation among determinants. Healthcare 5.0 can make it possible to establish a comprehensive personalized healthcare service (CPHS) for

patients and improve their long-term health. Figure 7 sketches the difference between partial and comprehensive health.

In the following subsection, we used an example use case scenario based on the CPHS.

1) EXAMPLE USE CASE SCENARIO

Figure 8 shows different health monitoring devices (like automatic blood pressure monitor, automatic blood glucose and blood sugar monitor, automatic heart rate monitor, and automatic insulin pump) that monitor different health conditions (like blood pressure, diabetes, heart, and cholesterol) of a patient. The monitoring devices share underlying health condition data collected during the data collection phase, for further processing. Later, the collected data is used by other applications to monitor and control different health conditions when required.

Currently, the applications monitor and control every monitoring device separately mainly because each device is manufactured for control and monitoring of a dedicated health condition whose details are in Table 4. However, this is not practical because, in reality, various health conditions are interdependent. For instance, a certain health condition (e.g., high blood pressure) could be a consequence of a side-effect of another specific health condition (e.g., high cholesterol). Therefore, we describe a use case scenario that aims to provide optimized and rigorous personalized health conditions of a patient through analyzing intra-dependencies among different health conditions of the patient. To this end, we consider the following two variations of the dependencies:

- One-to-Many (1–*), where a health condition may affect none or many other health conditions, e.g., common cold, fever.
- Many-to-Many (+−+), where various health conditions affect various other health conditions, e.g., arthritis, diabetes and epilepsy.

As sketched in Figure 8, in our example use case, the data is first collected from different monitoring devices and then used to analyze dependencies among the monitored health conditions as follows:

- No-dependencies - each health condition data is used to determine if it appropriately characterizes the underlying health condition. For instance, common cold or fever has no long-term effects on a person's blood glucose/cholesterol levels.
- Dependencies - data from different health conditions determine side-effects of various other health conditions. Which results in getting other health conditions. For instance, medical conditions interact with one another in the following ways:
  - One medical condition might make another worse like someone with arthritis who finds difficulty in exercise got a heart or lung problem.
  - One medical condition could start other serious medical conditions like diabetes contributes to cardiovascular disease, high blood pressure that leads to a heart attack or stroke.

- May clash with each other, making one ineffective or producing side effects.
- Treating one medical condition might make the symptoms of another worse or may produce a new or previously hidden health condition [41].

Based on the identified dependent health conditions, their current treatment, and other associated patient's routine (e.g., exercise and food), control applications determine a target personalized health condition by optimizing the involved health conditions. To this end, the application issues appropriate control alarms manipulated automatically or semi-automatically to establish the health condition.
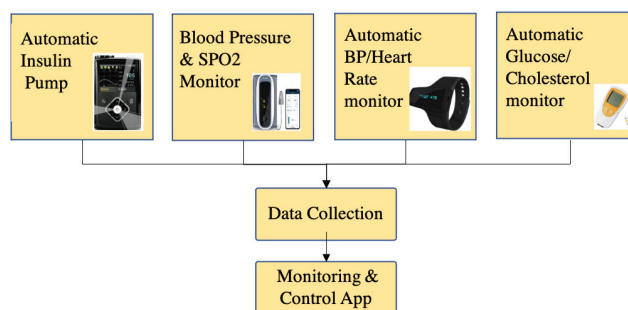

FIGURE 8. Example use case scenario.

In the following subsection, we define the key requirements for establishing CPHS.

B. KEY REQUIREMENTS OF CPHS

Healthcare 5.0 is the emergence of digital wellness [42] and it aims to provide personalized healthcare services by integrating cyber (e.g., monitoring/control) and physical (e.g., biological) processes/components of the service. Their integration helps to develop personalized healthcare services that are autonomous supporting automatic control of healthcare services by remotely monitoring the health conditions. Since these services are part of the critical application domain, therefore such services should meet certain critical requirements [43] for service operations that are given below:

1) **Reliability Requirements:** need to address the following key attributes:

- **Confidentiality:** ensures that only authorized users and devices can use medical data.
- **Integrity:** ensures the data completeness and accuracy in the entire communication to avoid wrong diagnosis and prescription.
- **Availability:** ensures the accessibility of medical data and devices to the authorized users at the time of need without any failure.
- **Privacy:** ensures that the privacy policies must be followed and any sensitive and private data must not be disclosed or shared without consent.
- **Data Freshness:** ensures that the physician or the system will get the recent data to rightly diagnose and prescribe and supports real-time response. For

TABLE 4. Health monitoring devices.

Things	Product Name	Vendors	Communication	Accuracy
Blood Pressure Monitor	Viatom Blood Pressure and SP02 Monitor	Viatom	Bluetooth	±3mmHg
Automatic Insulin Pump	MiniMedTM 640G	MiniMedTM	Radio	±5% to ±20%
Blood Cholesterol Monitor	Accutrend Plus	Roche	Biosensor	-1.29 - 0.98
Heart Rate Monitor	Viatom Sleep Oximeter With Vibration	Viatom	Ring Sensor	2 bpm or ±2%

example the fresh data for blood glucose level in fasting to set the right amount of insulin.

- **Security:** ensures the three fundamental security elements, i.e., "privacy", "integrity" and "accessibility".

2) **Resilience Requirements:** IoT-based healthcare system includes the following [43] requirements:

- **Protection,** involves:
  - **Self-healing:** is the process in which the system identifies the failure of medical devices and is able to recover the software and hardware automatically without any data loss.
  - **Self-optimizing:** is the process in which the system will improve its performance, quality of service and can automatically optimize resource consumption like energy, memory, etc.
  - **Self-protecting:** is the process in which the system automatically protects itself against harmful attacks and generates alarms in case of any suspicious/failure event.
  - **Self-configuring:** is the process in which the system automatically installs, configures, and integrates itself to eliminate system's flaws.
- **Safety,** ensures the safety of data and devices (i.e., the safety of the patient as well as of the involved cyber and physical components).

3) **Personalized Requirements:** These are the characteristics that are personalized to every patient and are a factor of response to the patient's health condition, immune system, and other underlying associated health conditions. Here are few such requirements:

- **Deep-analysis:** ensures that each health condition of a patient is determined by analyzing various aspects of the condition including, mechanical and biological processes of the condition monitoring. The immune system of different patients may respond differently against the same disease. Furthermore, different medical devices used for monitoring health conditions may have different characteristics, e.g., error rates.
- **Coordinated-healthcare:** ensures that the personalized health condition is resolved as a comprehensive health condition, and is possible through deep-analysis of each health condition of the patient and by identifying various (mechanical and

biological) dependencies among different health conditions of the patient. This helps to identify the strictly personalized health condition of the patient.

IV. REFERENCE ARCHITECTURE FOR IoT BASED HEALTHCARE SYSTEM

The word Internet of Things (IoT) is a combination of two words Internet and Things. Every object capable of connecting to the internet is considered as Thing, which includes smart devices, sensors, and context-aware objects that can communicate and are pervasive. Considering IoT as fully pervasive, IoT devices must possess the following three basic qualities:

- **Ability to Sense**: IoT devices must carry the ability to sense and combine the sensed data. For example, in the healthcare field, blood glucose, heart rate, body temperature, cholesterol level are sensed and aggregated using different specific biosensors. The data aggregation is autonomous.
- **Communicable**: After sensing and aggregating, IoT devices should be able to transmit data to the various desired data centers by using different communication mediums (i.e., Wireless Technologies, Mobile networks (3G, 4G, 5G), wireless local area networks (WLAN), wireless sensor networks (WSNs), and Mobile Adhoc Networks (MANET), etc.).
- **Actionable**: The aggregated data alone doesn't make any sense so, in the case of responsive devices IoT devices must be able to process the data in order to take some action. For example, if a patient's pulse rate or blood pressure level is sensed and communicated, alone this data is useless unless some processing technology is applied and the system finds that if it exceeds/falls behind from normal range. IoT systems also need to be capable to send automatic alerts to healthcare providers for further interventions.

We consider HIoT architecture based on three tiers. This three-tier structure consists of the Things layer followed by the communication and application layer. The description of the HIoT system and its operational and control functions is shown in Figure 9

In the following sub-sections, we analyzed the three layers of the IoT systems. In each sub-section, we

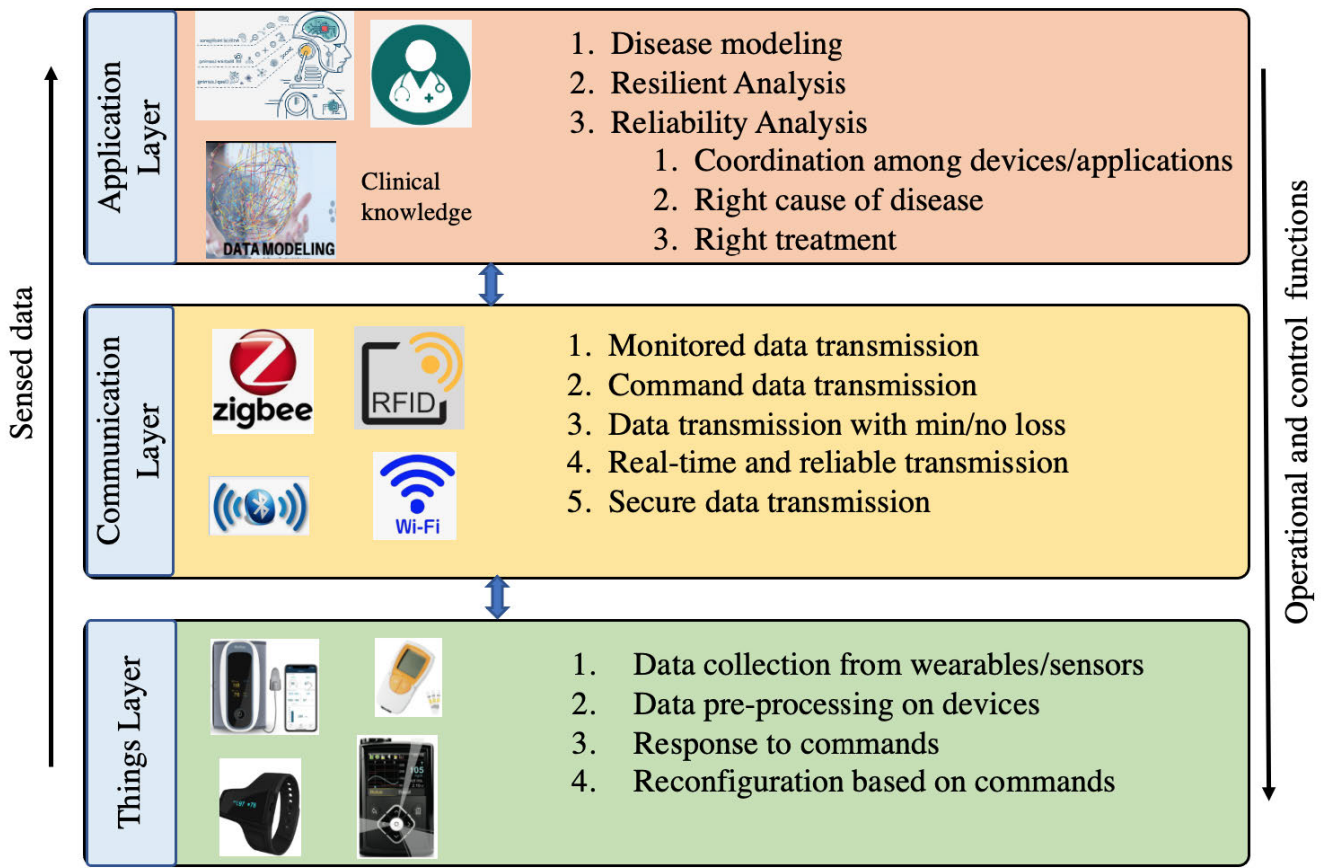- discussed a general overview of the layer,

FIGURE 9. HIoT system architecture.

- identified key challenges to establish the identified requirements of HIoT (e.g., reliability, resilience, and personalization),
- analyzed current approaches (AI/non-AI-based) and to address the above challenges, and
- identified the challenges as research gaps that have not been addressed adequately.

A. THINGS LAYER

IoT devices are seamlessly integrating into healthcare and have reformed the healthcare industry with their multiple healthcare monitoring devices and applications. IoT-based solutions like smart sensors, wearable devices, and smart health monitoring systems play significant roles in developing healthcare systems (smart hospitals, mobile healthcare (mHealth)), and the healthcare industry. Things layer [44] in HIoT, are sensing systems and devices that record the different values observed from different sources (i.e., devices monitoring patient's different body parts or health conditions) based on the application. Things layer consists of different devices and Things, that include:

- **Sensors,** whose aim is to sense/detect the physical quantities like temperature, pressure, smoke, light, etc., and then convert it into desired output in the form of

the electrical signal to measure the applied physical quantity. Sensors are further categorized into:

- **Biosensors** are analytical devices used in detecting the presence or concentration of a biological analyte, such as a biological structure, molecule, or a microorganism in the living body. Biosensors usually consist of three parts:
  * **Chemical Component**, whose job is to recognize the analyte and produce a signal,
  * **Transducer**, that converts this signal to an electrical signal and
  * **Reader Device** where this signal is displayable.

Figure 10 sketches biosensor operation and its main components.

Biosensors play a vital role in the medical field, health condition monitoring, clinical analysis of different health conditions, and diagnostic applications. They are advantageous over the lab equipment due to many reasons. Some of them include small size, low cost, quick results, reusable, and avoiding contamination. A comprehensive list of biosensors based on their working mechanism is shown in Figure 11. Further different types of biosensors, their details with their working
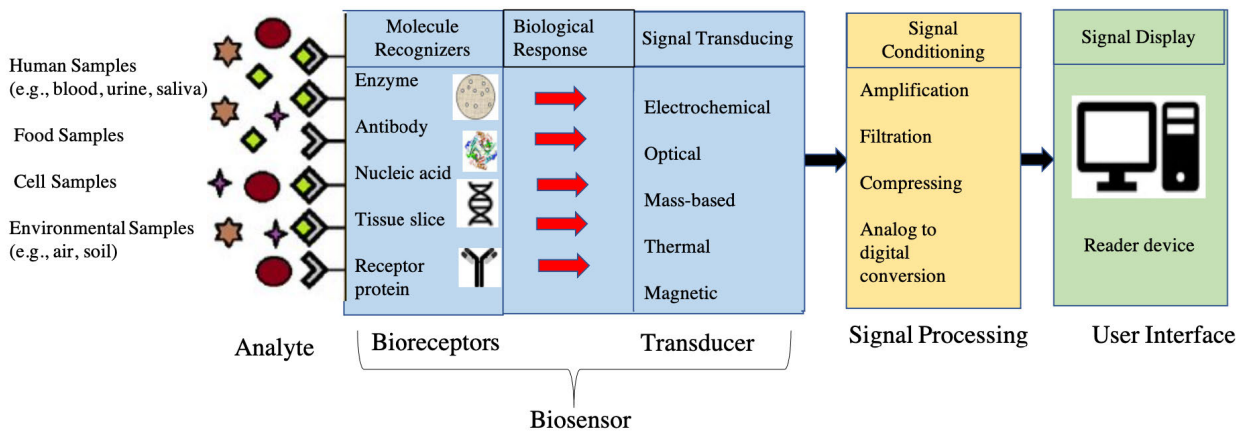
FIGURE 10. Workflow and components of biosensors.

principles and the diagnosis are shown in Table 5. These sensors aims at detecting disease-specific data from a patient's body.

- **General-Purpose Sensors** like temperature sensor, pressure sensor, proximity sensor, accelerometer and gyroscope sensor, infrared (IR) sensor, optical sensor, gas sensor, smoke sensor, and many more. These sensors aims at detecting various environmental conditions required for a patient's health.
- **Wearable Monitoring Devices** are the sensors that are worn anywhere on the human body in the form of some object that allows continuous or intermittent monitoring of physiological signals. They play an important role in healthcare, industrial process control, online control, offline control (distant and local), military applications, and continuous environmental monitoring. Some examples are ring sensor, smart shirt, heart rate monitor, blood pressure monitor, blood sugar monitor, stress monitor, smartwatches, textiles, glasses, patches, etc. These wearable biosensors are used for different applications e.g.,
  1) **Ring Sensors** are used for:
     - Wireless supervision of people during hazardous operations in the military during fire fighting.
     - In an overcrowded emergency department.
     - In cardiovascular disease for monitoring the hypertension.
     - For chronic surveillance of abnormal heart failure.

     The main advantages of using wearable monitoring devices are:
     - Continuous monitoring,
     - Detection of transient phenomena,
     - Promote further diagnostic and therapeutic measures,
     - Easy to use, flexible, and
     - Reduces hospitalization fee.

Considering their use Wearable devices are expected to reach a market value of €24.4 billion globally by 2023. There have been various developments in wearable devices. In [45] the authors presented a novel ring sensor for the continuous measurement of sympathetic nervous system activities. They successfully tested it on different age groups and got accurate results compared to the state-of-the-art open-source devices. The technology used by wearable gadgets is with low processing capabilities. Some examples are Google Glass and Smartwatch. Mobile devices are used as the computation source to increase the impact of these wearables technology. However, in terms of device security and privacy, this wearable technology is not as mature as it needs to be. These devices are vulnerable to attacks due to the security and privacy issues where due to the low processing power, the developers can't use complicated security mechanisms and algorithms [46]. Some of the disadvantages of wearable monitoring devices are

- Initial cost is high
- Limited number of physiological parameters for monitoring
- battery life is short

  The battery life of wearable monitoring devices is addressed In [47] where authors used the original dictionary-based technique where battery life for these devices used in healthcare is achieved by compressing the biosignals, and this compression is achieved by building and maintaining a dictionary at run time.

2) **Medically Implanted Devices/Sensors** are used in the human body in the following ways:
   - For replacing a missing biological structure,
   - for supporting a damaged biological structure, and

TABLE 5. List of Biosensors with types, principle and diagnosis [48].

Sensor Type	Sensor Name	Diagnosis	Principle	Portability
Electrochemical [49]	Glucose Oxidase Electrode Based Biosensor	Analysis of Glucose in Biological Sample	Electrochemistry using Oxidation	No
Optical/Visual/ Fluorescence [50]	Stilbene-420	eye glasses, biosensing	Optical/Visual/Fluorescence	No
Microbial [51]	Microbial Fuel Cell-based Biosensors	Energy production and environmental sensing	Optical	Yes
Electromagnetic [52]	Quartz Crystal Biosensor	TNT Explosive Detection	Electromagnetic	No
Electrochemical [53]	carbon-based screen-printed electrodes	water quality monitoring	Electrochemistry	No
Enzyme-based [54]	Glucose Oxidase Biosensor for Diabetes	Diabetes	oxidation of Beta-D-glucose	Yes
Amperometric Biosensors [55]	Nitrite Biosensors	Environmental Analysis of Nitrate, Nitrite, and Sulfate	Enzymatic	Yes
DNA Biosensors [56]	Electrochemical DNA Biosensor	Detection of Human T-Lymphotropic Virus-1	differential pulse voltammetry (DPV)	Yes
Enzyme-based [57]	Thiol Biosensor	Highly Selective Detection of Glutathione	Electrochemical	Yes
Enzyme-based [58]	Implantable Glucose Biosensor	Continuous Glucose Monitoring	RF sensor	Yes
Enzyme-based [59]	Cholesterol Biosensor	Cholesterol	Single-Mode Fiber (SMF) and a Hollow Core Fiber (HCF)	Yes
Enzyme-based [60]	Nitric oxide Biosensor	Detecting NO Gas	Conventional Wire Bonding Technology	Yes
Enzyme-based [61]	Superoxide Anion Radical Biosensor	Evaluating the photosensitivity of colorful wastewater	Chemical Reaction	Yes

− for enhancing an existing biological structure

using biomedical material tissues, active implant electronics, and transplanted biomedical tissues. Some of the examples of medically implanted devices are cochlear implants, automatic insulin pumps, pacemakers for cardiovascular diseases, retinal implants, artificial heart, cardiopulmonary bypass, and many more.

The above-mentioned sensors and devices collect data from the patient's body and in some cases after small processing transfer this data to the data center where this big data is analyzed. In some responsive sensors, the devices monitor the related body parameter and after processing perform the operation for the body like in smart automatic insulin pumps, the sensors check the blood sugar level of the patient in specific time intervals and based on the disease modeling of the device performs operations and automatically inject insulin into the body of the patient. We have highlighted key challenges of the Things layer that hinders key requirements of HIoT as identified in the Sub-section III-B. Furthermore, we have analyzed current approaches (AI/non-AI-based) to address the challenges. Additionally, we have also identified the challenges as research gaps that have not been addressed adequately. In the following, we have discussed the above for each requirement, namely reliability, resilience, and personalization, in order below.

1) **Reliability:** Reliability is the probability of a component or a system reaching specific performance

standards and producing the desired output in certain environmental conditions for a specific time duration [62]. In other words for IoT devices, reliability can be defined by considering the following three requirements [63].

- Perform a required function (i.e., Things are performing their required functions as expected, which is mainly sensing of various parameters).
- Perform the function under stated conditions (i.e., Things are functioning in the desired setting/configuration and environment)
- Operation for a specific time (i.e., Things are automatically functioning at a configured time for a specific time)

Reliability is one of the main challenges in sensor technology and in the more sensitive systems like healthcare reliability is of vital importance. The major challenges that hinder reliability of Things layer include:

- Constrained nature of the Things that contains battery, memory, and computational capacity [63], [64].
- Conditions of the operational environment (e.g., heat, freezing temperatures, mechanical or spontaneous wear, vibration, and moisture) [65].
- Tendency of sensors to "fail-dirty" (a phenomenon in which the sensor continuous to send fallacious information after some failure) [66], [67].
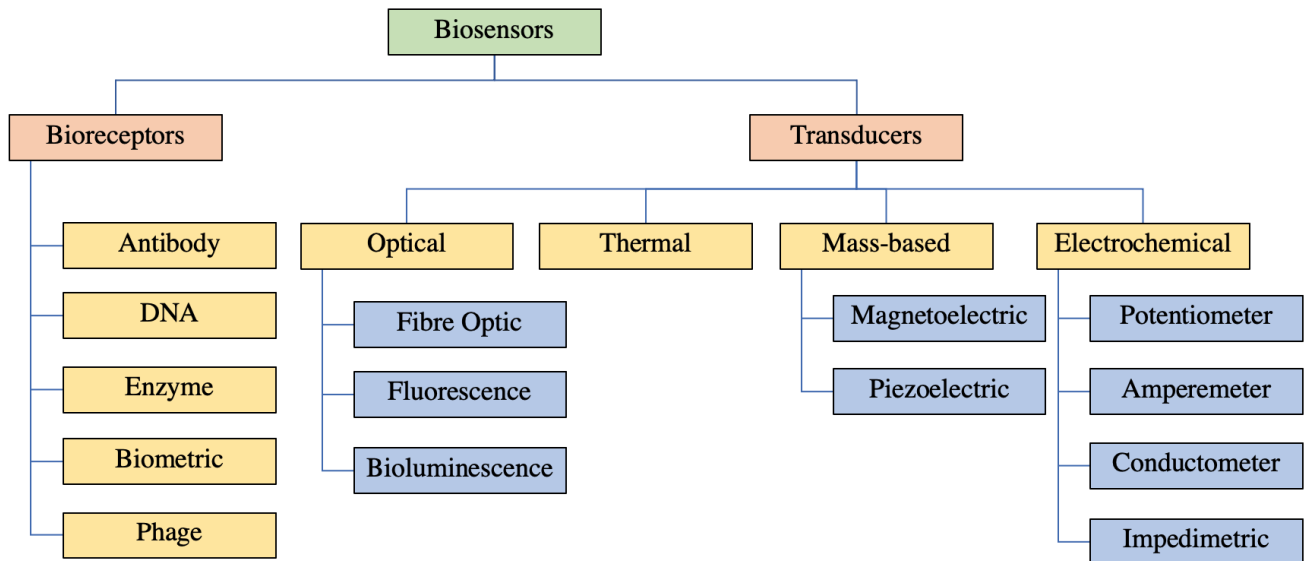
FIGURE 11. Typical nomenclature of biosensors.

In [68] the authors presented a smart and secure framework for the hospital environment using the Internet of Things (IoT) and Artificial Intelligence (AI). The presented system solved information system, treatment, diagnosis, patient monitoring, and record maintenance problems effectively. According to [69]–[71] AI-based algorithms are able to process huge amounts of data that are collected from different smart IoT devices within split seconds and predict the result, these predicted results along with the electronic health reports (ERHs) can be further analyzed by medical partitions. AI-based algorithms are able to think and detect illness faster with better accuracy and can assist the practitioners about the possible illnesses that can cause serious health problems in the future and can suggest possible treatment and medications for these diseases. In [72] artificial neural networks (ANN) are used to analyze urine and blood samples, as well as track glucose levels in diabetics, determine ion levels in fluids, and detect various pathological conditions.

Above mentioned challenges are addressed in different ways. For instance, [11], [73] proposed solutions to improve the reliability of sensors by making sensors capable of obtaining and providing reliable and accurate data. Evaluation of sensor reliability involves statistical or probabilistic data that multiply the reliability estimate. According to [74] the development of "smart sensors" can improve the reliability of the sensors. Current devices operating at the Things layer are not rigorously reliable to support real-time and critical operations of HIoT. For instance, some devices suffer from discrepancies by design [75], e.g., the error rate of blood pressure monitor. Similarly, the others may

be faulty either due to their maligned software (e.g., as a result of security attacks) [76], [77] or for some mechanical failure (e.g., as a result of mishandling of the device by an elderly patient). Moreover, such devices also fail to operate reliably due to their limited resources, e.g., battery life of sensors, signal strength, memory, and computational capacity [63], [78], [79].

2) **Resilience:** Resilience is the capability of systems to continue their normal operations and vigorous response in case of any unexpected or unpredicted situations. The importance of resilience multiplies in sensitive systems like healthcare where the continuity of the system is desirable from diagnosis to treatment and follow-up. Gaps in the continuity of care threaten a patient's well-being and cause adverse events. According to [80], resilience is two-fold; a system must be sound enough against attacks (that is in the first place be able to obstruct most attacks) and it must be able to go back to a safe state after any occurred attack. Abnormal operations at the Things layer occur due to several reasons. Some of them are as under:

- Hardware failure (e.g. sensors failure, failure of the control unit of IoT due to hardware and/or software, etc.) [81], [82].
- Failure of cloud services [83], [84] that may include failure of software, hardware, scheduling, service, power, and denser system packaging.

There have been some efforts to deal with the different issues of IoT. In [85] the authors focus on the IoT healthcare infrastructures, failures of components (hardware, software), and complete systems. The reasons for their failure may vary depending upon the healthcare IoT infrastructure. According to [86]

important challenges that hinder the safety and failure-free execution of IoT are as under:

- Capabilities and technical specifications of IoT's.
- Geographically dispersed deployment.
- Lack of security policies.
- Diverse attacks on IoT, and management of security patches.

So far, various approaches have improved the resilience of healthcare IoTs [85], [87]–[90]. In [87] authors proposed an intelligent collaborative security model to minimize the security risks, but the possible failures of IoT components and systems are not handled and their influence on the infrastructure is still unsolvable. In [88] the authors used traditional techniques of safety and violence for describing failure and misuse cases.The works in [85], [90] proposed the Markov Queuing approach for taking into account the safety and security issues of healthcare IoT infrastructure. In [85] the author proposed the Markov model that considers possible failures of healthcare IoT systems as well as recovery procedures.

In [82] the authors proposed a lightweight security scheme for ensuring transmission resilience and information confidentiality in the Internet-of-Things (IoT) communication. In their proposed system a single-antenna transmitter communicates with a half-duplex single-antenna receiver in the presence of a sophisticated multiple-antenna-aided passive eavesdropper and a multiple-antenna-assisted hostile jammer (HJ). The proposed system is demonstrated using simulations. However, some technical challenges like network synchronization and interference cancellation need to be addressed in experimental validation. In [91] the authors designed a novel blockchain-enabled authentication key agreement protocol BAKMP-IoMT for the internet of medical things (IoMT) environment that provides secure key management between implantable medical devices and personal servers, and also between personal servers and cloud servers. The proposed design stores data using blockchain and this data can be accessed by the users in a secure way using cloud service. The developed tool provides resilience against different types of possible attacks.

Current devices operating at the Things layer are not resilient, i.e., they fail to recover in case of any failure or physical damage. AI and blockchain-based technologies provide data transmission and storage resilience. The devices support limited hard resilience. They support resilience either by restarting the device in case of software failure or by replacing the device in case of mechanical failure/damage.

3) **Personalizing:** With the exponential growth of commercially available wearable devices, the concept of IoT-based personalization healthcare services is well-established and well-liked. These healthcare services use a set of interconnected devices and create an IoT-based healthcare network that is capable of observing and recording multiple types of health related data. After collecting data, different healthcare activities are performed such as monitoring, diagnosis, treatment, and remote surgeries [92]–[94]. In [95] the authors developed smart socks using textile-based triboelectric nanogenerator (TENG). The authors developed Artificial intelligence (AI)-based algorithms, for gait analysis and provide detailed information of multiple triboelectric socks users. It helps to identify various health conditions and activities of users for smart home and healthcare applications. In [96] the authors tried to access the capabilities of AI for predicting congestive heart failure for the COVID-19 patients. AI can help to provide advanced cardiac treatment, and to analyze-/measure the functioning of the human heart.

According to [92], [97] the major challenges for personalised healthcare are:

- Data privacy and security,
- handling big data (as some healthcare sensors/wearables are working 24/7),
- healthcare application are inadequate and may suffer:
  - Low quality of data deliverance.
  - Performance analysis.
  - Data storage.
  - Privacy prevention, and standardization.

The authors used different approaches to address the above-mentioned challenges like cryptographic techniques for attaining data privacy and security, cloud storage system to handle huge healthcare data and smartphone-supported self-monitoring sensors for better quality performance. Current devices operating at the Things layer provide limited personalized healthcare services. For instance, they can be configured to monitor a specific health condition (e.g., chronically ill patients, active and assisted living, dementia, diabetes, breathing problems, etc.) of a patient in a specific environment (e.g., smart homes, care centers, etc.). Consequently, Things layer devices are not reliable and resilient to address key requirements of CPHS. For instance, they fail to reliably provide continuous monitoring of a patient's health which may threaten the patient's life. Furthermore, the devices also fail to support CPHS, as they are technologically personalized (i.e., for specific medical conditions (like blood glucose, blood pressure, heart rate, etc.), and are not clinically personalized (i.e., unaware for the other associated medical conditions of the patient). AI/ML-based approaches provides personalization in specific environment [96] and for specific diseases [15].

B. COMMUNICATION LAYER

The communication layer is considered as the spine of the IoT systems [98]. IoT devices generate a large amount of continuous data that is challenging to store and communicate [99]. All the data from the Things layer is transferred

to the application layer through the communication layer. A suitable communication medium is required to transfer the data from all the nodes of the Things layer to the other layers of the system. The communication medium could be wireless (WiFi, Bluetooth, RFID, 5G, etc.) or wired (Ethernet, USB, etc.) based on the designed communication protocol. Figure 12 shows the communication medium classification according to connectivity in an IoT system. The major requirements for IoT communication in order to set up a successful healthcare 5.0 system include energy efficiency, range, cost, reliability, security, and scalability. Real-time data collection and data processing are carried out at the communication layer on IoT platforms and in information systems [99].
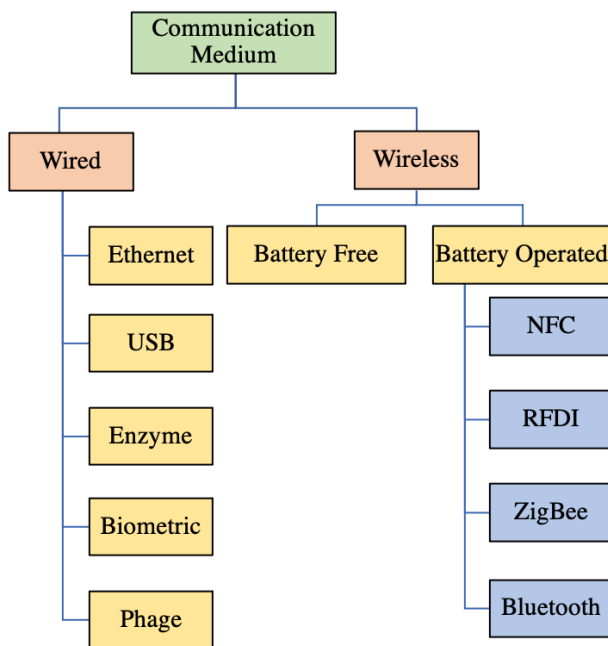

FIGURE 12. Classification of IoT communication mediums.

As the communication layer in an IoT-based healthcare system is considered the backbone of IoT communication, it inherits all the problems of the communication network. Analyzing the communication layer problems, in the following, we

- highlighted key challenges of the communication layer that hinders key requirements of HIoT as identified in the Sub-section III-B,
- analyzed current approaches to address the above challenges, and
- identified the challenges as research gaps that have not been addressed adequately.

We discussed the above for each requirement, namely reliability, resilience, and personalization, in order.

1) **Reliability:** According to the recent research [100] there are two forms of network reliability challenges, which are:
   - Enhancement of QoS in the network

- Evaluating the reliability functions for networks

There have been various attempts for improving the reliability of IoT networks through enhancing QoS parameters and by quantifying components based on the monitoring. In [101] the authors presented micro services QoS-aware middleware that monitors response time, throughput, availability, reliability, and cost parameters. In [102] authors used the Generalized Stochastic Petri Net (GSPN) approach for reliability modeling. The mathematical model used by them calculated the reliability of failure rate, consumption time, response time, and repair times. In [103] the authors proposed a gateway redundancy model which reduced the RTT (return trip time) as the performance metric and proposed methodology lowers the return time to 1% from 14% during fault conditions. In [104] the authors quantified some QoS metrics, like delay throughput, and packet loss. In [105] the authors proposed a general model for a QoS-aware IoT infrastructure, that only deals with latency and bandwidth. In [106] the authors provided an analysis of the role of fog computing, cloud computing, and the Internet of things for mitigating storage facilities related to the data of the patients and minimum capital investment on computing for uninterrupted context-aware services to the end-users. The authors proposed a three-layer patient-driven Healthcare architecture for real-time data collection, processing, and transmission. In [107] the authors' combined packet replication with modulation diversity using multiple IEEE 802.15.4g SUN modulations for the evaluation of the benefits of improving communication reliability. Their results showed a significant increase in packet delivery ratio (PDR), that enhance the reliability of SUN networks for industrial applications. In [73] the authors presented a framework for handling reliability in IoT based on the TCP (Transmission Control Protocol). The framework calculates delays, failure states, and re-transmission of the data. In [108] the authors proposed a novel approach that uses using machine learning and multi-objective optimization (moo) for the software-defined network (SDN)-enabled adaptive and reliable communication in an IoT-fog environment. The authors successfully evaluated reliability using ML-based algorithms, while the "moo" algorithm is used to find the Pareto-optimal paths. The proposed approach is more faster and reliable compared to the other existing ones.

In [109] the authors have provided a comprehensive framework to provide optimal solutions for privacy preservation, and energy optimization for researchers and practitioners in a better understanding of 5G infrastructures. The authors evaluated the proposed framework using case studies and mathematical modeling.

The afore-mentioned research has some limitations:
- The services are not scalable.

- Reliable performance only at a specific layer of the network like the edge layer.
- Limited view of network performance like limited to only TCP.
- Only specific for specific parameters of QoS (e.g., delay, throughput, packet loss, etc.).

So far, there is no combined approach which deals with reliability considering both QoS and quantifying component parameters. Being wireless, current communication infrastructures (e.g., media, protocols) used in HIoT are not reliable to support real-time and critical operations of CPHS. Due to interference, delays, and loss of data in wireless communication, data integrity becomes a serious problem from CPHS point of view mainly because a small variation in data can have significant consequences on a patient's health condition, e.g., a small error in blood pressure monitored values may not have a significant impact on the health condition, while a similar small error may have a significant impact on the health in case of monitored glucose values. Furthermore, to support continuous monitoring of health conditions requires high availability of the communication network, which is not the case in current wireless communication. However, 5G aims to support reliable communication [109], [110] through ultra-low latency, high bandwidth, ultra-high reliability, reducing interference, and enhancing QoS. AI/ML-based approaches provide more faster and reliable communication in IoT-fog environments.

2) **Resilience:** Analogous to the Things layer, the resilience of the communication layer can be realized as the capability of communication systems to continue their normal operations and vigorous response in case of any unexpected or unpredicted situations. To support real-time resilience for IoT based healthcare systems is very challenging mainly because the resilience of such communication system arise from the complexity of failures, namely failures of

- communication devices (e.g., router) or
- communication network (e.g., wireless media, protocol).

Former are partially resilient through reconfiguration, when current configurations get maligned but do not support resilience in case of any other mechanical failure. While the latter does not support resilience, for instance, any interference in wireless media and vulnerability in the communication protocol is not recoverable on the fly. Recently, various approaches have been proposed to support resilience in IoT-based communication networks. For instance, in [111]–[113] authors have proposed different Cloud and Edge-computing-based mechanisms to support the recovery of various network failures in IoT networks including DoS attacks. However, they are limited in supporting only communication network failures due to

denial-of-service (DoS) attacks and fail to support operational failures of communication devices in the face of other security attacks. Furthermore, there have been some efforts [114], [115] that introduce resilient aware architecture and overlays to support device failures in the face of security threats. However, these approaches are retrospective, i.e., they are only resilient in known scenarios and fail to provide resilience in situations that are either variant of the known scenarios or different from the known. In [116] the authors proposed secure demand-side management (DSM) engine that uses machine learning (ML) for the IoT-enabled grid that is responsible to preserve the efficient utilization of energy based on priorities. The proposed DSM engine reduces the utilization power of smart grids and is less vulnerable to intrusions. In [117], the authors designed an authenticated key exchange (AKE) protocol that can resist side-channel attacks and enhance security and privacy in E-Health applications. The proposed protocol provides stronger security and higher efficiency compared to similar protocols in IEEE 802.15.6 and Bluetooth 5.0.

Current communication infrastructures (devices and network) are typically not resilient, e.g., they fail to automatically recover in case of any soft (i.e., software/configuration failure/malfunctioning) or hard failure (i.e., hardware/device failure). AI/ML-based approaches can provide resilience by preserving the efficient utilization of energy based on priorities. They partially support resilience, for instance, soft resilience through self-configuration and hard resilience through configuring an alternative interface. However, these resilience methods hinder data integrity due to failure in recovering the loss of pre-configuration/failure data.

3) **Personalization:** The Communication layer supports personalization by providing various personalized communication networks (e.g., Wireless Personal Area Network - WPAN, Wireless Body Area Network - WBAN, and Internet of Medical Things - IoMT) that connect various medical devices of an individual patient. Although these networks support data and communication protection among personal devices, it fails to protect data and communication when these networks interact with external networks (i.e., Internet) for monitoring and analysis of patients' health conditions. For instance, in [118]–[120], various personalized communication mechanisms have been proposed that enable secure transmission of information among various medical devices. However, these approaches are limited in enabling on the fly integration and communication of new devices (e.g., IoT medical devices from different manufacturers supporting different communication protocols), and in protecting the end-to-end transmission of data among external healthcare agents (e.g., practitioners, carers,

and nurses) that involve other networks (e.g., Internet, LAN, and WAN).

Contemporary IoT-based communication infrastructure achieves personalization through supporting customized communication configuration for required healthcare services. For instance, 5G aims to support the traffic-free transmission channels for real-time data exchange among HIoT components to support emergency medical services. Furthermore, personalization can also be supported using personal clouds to prioritize the desired services.

Consequently, the communication layer is not reliable and resilient to address key requirements of CPHS, for instance, the current communication infrastructure fails to reliably exchange data for continuous monitoring of patient's health which may threaten the patient's life. Furthermore, the communication also fails to support CPHS, as they are personalized in a way that supports traffic-free transmission channels for dedicated services that are not stateful, i.e., the channels are not aware of the significance/semantics of the transmitted data generated through monitoring different medical conditions of the patients.

C. APPLICATION LAYER

The application layer communicates the users with the IoT/Internet of Medical Things (IoMT) platform directly and focuses on providing high-quality services in healthcare. IoMT is a connected infrastructure of devices, software, hardware, and services. With the advancements in connectivity, their use is exponentially increasing. These are used by healthcare professionals for processing and analyzing data for decision-making and patient treatment. In hospitals, the IoMT is typically about increasing patient safety and/or optimizing processes. It enables practitioners to work together across disciplinary boundaries to carry out individualized patient care. The goal of the application layer is two-fold, it provides:

- **Monitoring Applications:** that process the data and supports decision making on one hand, and
- **Support Applications:** that are mare interfaces to operate various health monitoring devices on the other hand.

Different approaches have been developed to support personalized healthcare services. Most of the approaches support personalized healthcare services by using various healthcare modeling and monitoring techniques as shown in Figure 13.

1) HEALTHCARE MODELING

There have been various efforts where personalization is addressed in the frame of healthcare modeling and monitoring. For instance in [45] the authors studied and investigated the modeling method for a cloud healthcare system. In this system, the authors used the telemedicine platform to share high-quality medical resources among big tertiary hospitals and small community hospitals. Their presented Petri net model used the colored Petri nets (CPN) tools for verifying

and analyzing the simulation process. The model describes the state of patients and the relationship between the medical process and resources in this cloud healthcare system.

In [35], the authors focus on the formal model Petri net where public-key encryption controls the security model. The authors successfully used Petri net mathematical modeling for solving graphical notations and minimizing the risks and overcoming the security risks in the healthcare industry. In [121] the authors focus on cloud-based healthcare systems. The authors presented Petri net for describing the relationship among medical processes and resources in their integrated healthcare system. The model solves the patient assignment scheduling problem using a greedy-based heuristic algorithm. In [122] the author employed machine-learning techniques to extract features from electrocardiogram (ECG) and informed hypertensive patients about their heart status during various activities. The experimental data were collected from a network of conscientious volunteers through a mobile crowd-sensing (MCS) application. However, the experimental data did not include the main diagnostic feature for hypertension that is blood pressure. In [123] the authors used an IoT sensor with artificial intelligence (AI) to predict the exact patient details such as fitness tracker, medical reports, health activity, body mass, temperature, and other health conditions. The collected patient details are processed according to the iterative golden section optimized deep belief neural network (IGDBN) which helps to choose the effective patient assistance system. In [124] the authors integrated Machine learning (ML) and blockchain technologies to solve the basic challenges of securely exchanging the big data that supports the analytics. The authors used ML algorithms like Naive Bayesian, k-nearest neighbor, and decision tree on the trained data to achieve higher accuracy in identifying the disease. In [125] the authors analyzed health data classification by tracking and identifying vital signs using state-of-the-art deep learning techniques and highlights the challenges (limited computational power, data redundancy) posed by edge intelligence. In [126] the authors surveyed the practicality of AI services for healthcare by healthcare professionals. The authors provide an analysis of the healthcare services that are using AI technology. According to the survey results majority of the health professionals are willing to use AI technology for supporting decisions.

2) HEALTHCARE MONITORING

In [127] authors explored and applied the IoT paradigm in the context of assisted living facilities (ALFs). They have designed and implemented a system capable of supporting the healthcare assistants in their daily livings while operating in ALFs with physical or cognitive disabilities. The system used wearables and mobile technologies to attain its goal. The system supports both inhabitants with cognitive disabilities with instant assistance through their wearable devices when required. The caregivers in potentially hazardous situations are alerted automatically. However, their focus is on one specific group with physical and cognitive disabilities.
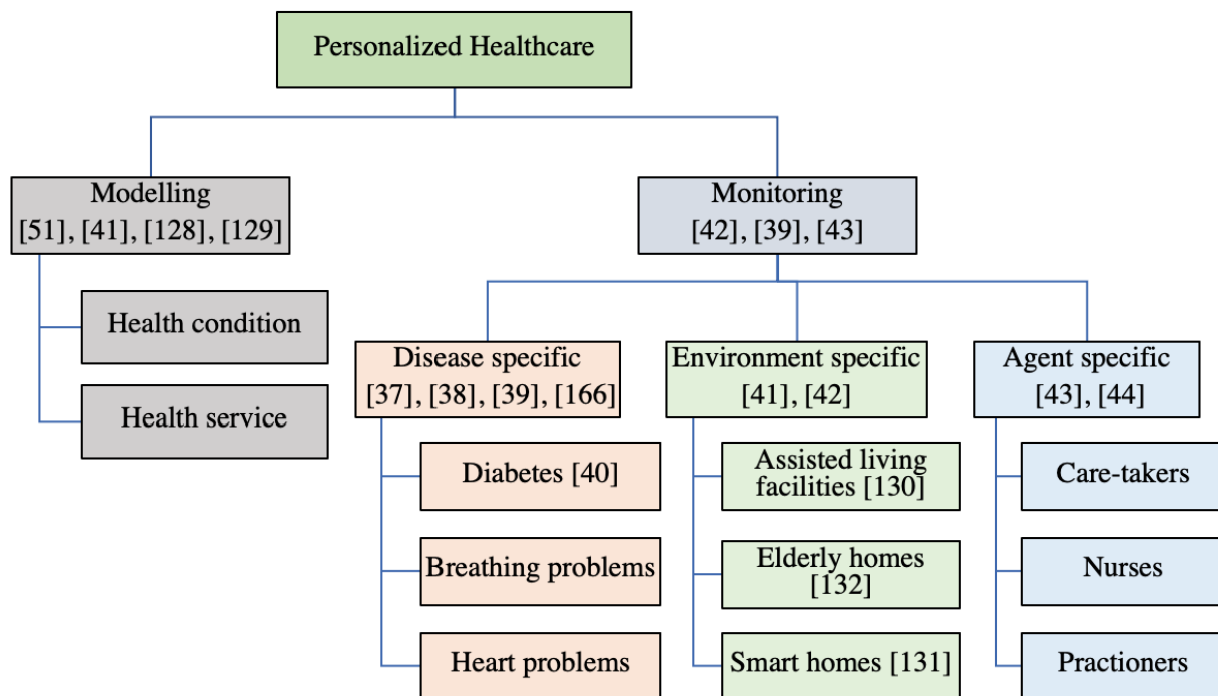
FIGURE 13. Classification of personalized healthcare modeling and monitoring techniques.

In [128], the authors exploited IoT technologies for enhancing healthcare in smart homes through patient identification and emotion recognition. They have automatically used images and emotions by using IoT infrastructure for helping healthcare in the smart home environment. Images were used for the detection of the right person to ensure to provide the right treatment while emotions are used as they play a very crucial role in the recovery process. They have used facial angles, gestures, and postures for emotion recognition. Smart watches and clothes with wearable sensors can be included in the smart home environment as a means of collecting physiological information which is then used for decision making.

In [129] the authors used AI-based predictive and prescriptive analysis by using open source technologies like Apache beam, Apache Flink Apache Spark, Apache NiFi, Kafka, Tachyon, Gluster FS, NoSQL- Elasticsearch, and Cassandra for data processing and used it for extracting useful knowledge that helps in decision making and patient's monitoring. In [130] the authors presented an architecture for continuous monitoring, ubiquitous connectivity, extended device integration reliability, security, and privacy support. The continuous monitoring is made feasible with the use of a proposed protocol called YOAPY. The efficiency and security are scalable integration of sensors that are deployed in the patient's personal environment. The focused group of patients is the patients with breathing problems. As the HIoT are continuously providing information about the health conditions of the patients, a large amount of data is collected

relating to the patient's health conditions which enable the use of advanced machine learning techniques. These techniques can be used to identify the information about user data, the effect of the treatment on patient's health, and monitor the progress [131]. In [132] the authors used machine learning (an AI technique) for the classification of skin lesions using a single convolutional neural network (CNN), trained end-to-end from images directly, using only pixels and disease labels as inputs. The classification was able to successfully diagnose skin cancer as efficiently as dermatologists. In [133] the authors proposed a smart healthcare system for heart disease prediction using ensemble deep learning and feature fusion approaches. The feature fusion method generates valuable healthcare data (excluding irrelevant and redundant features) from sensors and medical healthcare records. According to [134] AI-based systems can significantly reduce delays while incorporating new best practices and tools, for new significant periodic revision of scientific and medical knowledge in healthcare systems and help to optimize output more quickly.

In [36] authors proposed a personalized self-served health-monitoring system for the elderly in the home environment by combining general rules with case-based reasoning (CBR) approach. The system uses health parameters such as blood pressure, blood glucose, weight, activity, pulse, etc., and applies general rules to classify individual parameters. Case-based reasoning is used to combine different health parameters which ultimately generates the overall classification of health conditions. The system successfully generates

feedback, recommendations, and alarms in a personalized manner. However, the system works only in the specific elderly home environment and for a specific age group. Moreover, the system uses rule-based reasoning (RBR) and case-based reasoning (CBR) for the classification of health conditions. Facts and rules are strictly categorized in RBR and require a strict Boolean match on the conclusions and suppositions while the real-world problems like healthcare problems are often fuzzy and do not match exactly with rule-based conclusions and suppositions while case-based reasoning has its limitations w.r.t, the representational scheme used for the cases in the case library, structure of case library,need-based,retrieval and similarity metrics, and adaptation.

In [37] the authors propose a multi-modal hybrid reasoning methodology (HRM) that integrates the rule-based reasoning, case-based reasoning, and preference-based reasoning approaches sequentially by exploiting guideline rules, past successful experience cases and personal preferences to generate personalized physical activity recommendations according to the user's needs and preferences. The authors had successfully facilitated the users with different wellness services. However, the used approaches are not exhaustive and are dealing only the wellness services at a personalized level but not the personalized health of the users.

In [34] the authors proposed a personalized healthcare monitoring system for diabetic patients by utilizing Bluetooth Low Energy (BLE) based sensors and real-time data processing. Real-time data processing utilizes Apache Kafka for handling incoming sensor data whereas MongoDB is utilized to store the unstructured sensor data. The authors successfully handled continuous data (e.g., Blood Glucose (BG), heart rate, blood pressure, weight, and other personal data) from the BLE-based sensor devices by real-time data processing. The authors used multi-layer perceptron (MLP) to classify diabetes patients. In [38] authors proposed a smart application that monitors the health status by an easy user interaction for the users with limited technological experience. To implement the system, authors combined the Wearable sensors such as the Angel Sensor (for data collection) with voice interactive devices, and the Amazon Echo (for voice interfacing). In [122] the author employed machine-learning techniques to extract features from electrocardiogram (ECG) and informed hypertensive patients about their heart status during various activities. The experimental data were collected from a network of conscientious volunteers through a mobile crowdsensing (MCS) application. However, the experimental data did not include the main diagnostic feature for hypertension that is blood pressure. In [123] the authors used an IoT sensor with artificial intelligence (AI) to predict the exact patient details such as fitness tracker, medical reports, health activity, body mass, temperature, and other health conditions. The collected patient details are processed according to the iterative golden section optimized deep belief neural network (IGDBN) which helps to choose the effective patient assistance system. In [132] the authors used

machine learning (an AI technique) for the classification of skin lesions using a single convolutional neural network (CNN), trained end-to-end from images directly, using only pixels and disease labels as inputs. The classification was able to successfully diagnose skin cancer as efficiently as dermatologists.

The afore-mentioned approaches lack in one or many of the followings:

- They establish personalized healthcare service through visualizing personalized data that is focused on monitoring a selective health condition (like for patients with breathing problems, diabetes mellitus). The systems provide security and privacy support but fail to monitor the comprehensive personalized health condition of the patient.
- They applied IoT environment in a specific context (like assisted living facilities, smart homes, cognitive disabilities). The system only assists the caregivers and inhabitants in hazardous situations but is unable to monitor the comprehensive health condition of inhabitants.
- They developed a system that is working for people with less technological experience by using voice interactive devices in combination with smart sensors like Angel sensors. The system works for specific health conditions like diabetes mellitus and is not able to monitor the comprehensive personalized health condition of the patient.

In the following, we have highlighted key challenges of the application layer that hinders key requirements of HIoT as identified in the Sub-section III-B, analyzed current approaches to address the above challenges, and identified the challenges as research gaps that have not been addressed adequately. We discussed these challenges for each requirement, namely reliability, resilience, and personalization, in order below:

1) **Reliability:** The main goal of healthcare applications is to derive various facts about a patient's health based on monitoring through collecting data about a patient's health conditions from respective medical devices. The derivations are later used by the practitioner, patient, or caretakers to control the patient's health. Therefore, the reliability of these applications strictly depends on the reliability of such derivations.

    Analogous to the Things and communication layer, the reliability of the application layer can be defined considering the following three requirements:

    - Perform a required function.
    - Perform the function under stated conditions.
    - Operation for a specific time.

    In the following different approaches have been established/ developed which address one or more reliability requirements of the applications layer. In [11] the authors developed the reliability of the healthcare system, investigated and quantified their influence of the component states (functioning levels

and failure) based on unified methodology. In [135] the authors investigated the long-range wide-area network (LoRaWAN) frames loss due to the channel effects. They designed a novel coding scheme that combines techniques from convolutional and fountain codes called DaRe that works on the application layer for data recovery and provides better resilience.

According to [136] reliably helps to deliver effective interventions in healthcare organizations.They proposed a model to improve reliability which includes interventions to improve by focusing on valid rate-based measures. They used the following interventions for improving the reliability of the healthcare system:

- Identifying evidence-based interventions,
- selecting interventions with the most impact,
- developing measures to evaluate reliability,
- measuring baseline performance, and
- ensuring that patients receive the evidence-based interventions.

In [137] the author examined an innovative approach that uses the combination of specific work practices and behavioral processes for detecting unexpected events and then operates in a nearly error-free manner. Furthermore, they explored that reliability-enhancing work practices (RewPs) help to improve the performance of the system by reducing errors. Also, the RewPs are directly and indirectly associated with fewer medication errors and patient falls. In [10] the authors used the features of decentralization of database and consensus in Blockchain technology to get highly accurate results in terms of machine learning with the security and reliability of Blockchain Technology.

In [11] the authors presented fingerprinting healthcare applications architecture based on network slicing that can provide reliability for s-health applications and services. The developed system obtains 90 percent accuracy assisting in network customization. In the article [138] authors include purpose, process, people, and management system as the important constructs which are required for highly reliable healthcare. The article also explores the reasons for the failures in improvements in healthcare and suggests rigorous training and continuous attention for updating the standards. In [124] the authors integrated Machine learning (ML) and blockchain technologies for solving the challenges of securely exchanging the big data that supports the analytics. The authors used some ML algorithms like Naive Bayesian, k-nearest neighbor, and decision tree on the trained data to achieve higher accuracy in identifying the disease. In [139] the authors emphasized the great significance of the convergence of IoT and AI. they elaborated the knowledge-enabled AI and data-driven AI, comparing its advantages and disadvantages throughout the IoT architecture, from the things layer through the communication layer to the application layer. The authors highlighted that

reliability in data transmission, security and privacy are open issues during the convergence between IoT and AI. In [140] the authors presented blockchain-based electronic healthcare record (EHR) using javascript-based smart contracts for the patient-centric design of a decentralized healthcare management system. The authors developed and implemented a prototype based on hyper ledger fabric that provided performance such as latency, throughput, resource utilization for varied scenarios, and control parameters.

2) **Resilience:** Analogous to things and the communication layer, the resilience of the application layer can be realized as the capability of applications (e.g., healthcare service monitors and controllers) to continue their normal operations and vigorous response in case of any unexpected or unpredicted situations. To support real-time resilience of IoT based healthcare applications is very challenging mainly because applications may fail due to:

- Inadequate and vulnerable design of applications (e.g., techniques that application employ (for instance, machine learning and AI), programming languages used to develop applications (for instance, Python and Java), to name a few), and
- inadequate and vulnerable applications' execution (e.g., data, network, and run-time libraries).

Former (aka design) failures are key threats to the resilience of healthcare applications being unrecoverable in real-time due to the time required to localize the failure and then fix it. Furthermore, design limitations (e.g., false alarms, bias, complex processing) of techniques (e.g., machine learning and AI) that are used in healthcare applications may lead to severe consequences resulting in life threats to patients [141]. Different approaches [142]–[145] have sketched various limitations of application techniques in healthcare and have devised ways to address them in a way that requires developers to handle various resilience concerns while developing such applications, e.g., dataset shift, accidental fitting of confounders, unintended discriminatory bias, generalization to new populations, and the unintended negative consequences of new algorithms on the health condition outcomes. However, these approaches are error-prone being manual, and do not ensure application resilience. More recently, model-driven approaches have been used to significantly improve the design of such applications to support resilience. For instance, in [146]–[149] various models have been proposed to design such applications that do not include different vulnerabilities and inadequacies supporting resilience by design. However, these approaches only support resilience in the known (via models) scenarios, and fail to recover from failures that are either variants of the modeled ones or different from them.

Latter (aka execution) failures are harder to recover mainly because they involve unseen incidents that take a lot of time to identify the incidents' cause and then to fix them. Furthermore, identification here is challenging because the execution environment involves very complex infrastructure most of which is a black box (e.g., communication infrastructure and IoT devices from different manufacturers and platforms and services from different providers). To this end, various monitoring techniques have been developed to detect such incidents at run-time and mitigation techniques that recover the application's failures in a way to minimize the impact of the incident. Current approaches [150]–[152] introduce different risk-based maintenance methodologies that enable recovery of healthcare applications making them resilient aware in certain scenarios against known threats. In [153] the authors presented a novel and resilient approach for improving the operational efficiency of computational cost by using approximate computing (AxC) that can significantly boost the efficiency for adopting AI-based applications and services. They presented a multi-tera operation per second (TOPS) AI hardware accelerator core that they built from the ground-up using approximate computing (AxC) techniques across the stack including algorithms, architecture, programmability, and hardware.

3) **Personalization:** Contemporary healthcare applications support personalization [154], [155] in one or more of the following different ways:

- Patient's self-organization of various health conditions,
- health condition and/or patient-specific gadgets and automated guidance.

The patient's self-organization is supported by developing applications [156], [157] that can be customized as per patient's requirements, e.g., goal setting, celebration, discovery, reflection, and coordination among others. However, these approaches do not support clinical personalization that requires clinical optimization of various health conditions to reduce health risk and to improve the quality of health/life of the patients.

Various gadgets (and associated applications) [158]–[161] have been developed to support the customized organization of various health conditions. These gadgets provide health condition-specific monitoring and control patiently. These approaches provide very restricted customization of gadgets for a specific health condition of the patient.

Recently, various ML and AI-based applications [162]–[166] have been developed that provide personalization of a specific health condition to the patient based on data collected from personal medical devices of the patient over long periods. However, the above-mentioned approaches are limited in realizing the personalization that is data-driven which suffers from false predictions resulting in a severe loss. In [163] the authors addressed the major issues such as explainability, liability, and privacy to mainstream AI in healthcare. Explainable AI, a new emerging discipline seems to be the solution for making machine decisions transparent, interpretable, traceable, and reproducible.

Consequently, the application layer supports either technological personalization or health condition-specific personalization to patients. This support is limited and does not provide clinical personalization of various health conditions of a patient in a way that reduces the health risk on one hand and improves the quality of life and health on the other hand. AI/ML-based approaches can be partially used at the application layer. These techniques can be used for health condition monitoring or for dealing with the patient data e.g., patient's history, treatment record, security of patient data, and progress about recovery. But for critical matters like diagnosis, treatment AI/ML-based techniques can not be implemented due to the explainability and trust of these applications. A lot of work is still in progress regarding the explainability and trustworthiness of AI.

V. RESEARCH GAPS

The research gaps in the IoT layers in the frame of comprehensive personalized healthcare services requirements are shown in Table 6. These derived gaps determine research challenges that are associated with different layers of the architecture and corresponding key requirements of healthcare. The identified gaps conclude that the current HIoT devices and applications monitor a specific health condition of patients [167] (e.g., insulin level, ECG level, and oxygen saturation monitoring devices) and thus are not reliable for a patient with multiple health conditions as they fail to provide reliable, resilient, personalized, and application-specific healthcare mainly because these applications,

- do not coordinate with other similar applications that monitor different health conditions of the same patient and as a result, fail to understand the health context of the patient, and,
- do not exchange information securely due to unreliable and heterogeneous underlying software and hardware.
- does not understand the effect and relation among different health conditions of a person.

The comparison of various smart healthcare approaches like AI-based, Machine learning-based, and deep learning-based is shown in Table 8. The comparison clearly shows that only few among the above mentioned approaches either partially support (i.e., indicated by half filled circle) or do not support (i.e., indicated by empty circle) personalization of healthcare services considering multiple health conditions of a patient. The above mentioned analysis of the CPHS requirements (i.e., reliability, resilience, and personalization) at different layers has been performed under the assumption that operations of the respective layers exhibit normal

TABLE 6. Research gaps for CPHS requirements.

Requirements IoT Layers	Reliability	Resilience	Personalization
Things	Discrepancies by design Maligned software Mechanical failure Limited resources	Fail to recover Limited hard resilience	Limited personalised healthcare services disease specific
Communication	No reliable real-time support No reliable support for critical operations No reliable data exchange	No automatic recovery in case of failure	Personalised support only in case of personal clouds
Application	False detection due to ML Not rigorous	Inadequate and vulnerable design of applications Inadequate and vulnerable applications	Support technological personalization Health condition specific personalisation

behavior, which is not true in practice due to emerging security threats to different layers. Therefore, we consider security as integral to the CPHS requirements that enable us to identify the security threats that affect the normal behavior of the layers. In the following section, we discuss various security threats to different IoT layers.

VI. SECURITY THREATS AT IoT LAYERS

Security threats at different IoT layers and their possible mitigation are shown in Table 7.

A. SECURITY OF IoT DEVICES

The increase in the number of modern IoT devices and their exponential use in healthcare systems has increased the risk of security-related issues and other vulnerabilities. As per [168] till 2025 number of IoT devices per second will rise to 152K. The emergence of Wi-Fi 6 and 5G networks provides higher data rates to support new applications and increases network capacity. They are exponentially scalable and will bring much better performance for organizations with the improvement in speed, latency, and scalability and will be ideal for indoor enterprise networks. The main reasons associated with security issues are as follows:

- The nature and sensitivity of the data which is communicated by medical devices.
- Complexity and data compatibility issues.
- Lack of attention towards security issues by manufacturers of medical devices.

Due to the above-mentioned reasons, security-related issues related to confidentiality, integrity, and availability (CIA) are increasing [43] for IoT devices.

These devices are not fully secure and face different types of physical attacks. Some examples of these attacks are as under [79], [169]:

- Node tampering.
- RF interference on RFID's.
- Node jamming in Wireless Sensor Networks.
- Malicious node injection.
- Physical damage.

- Social engineering.
- Sleep deprivation attack.
- Malicious code injection.

According to [170], following security issues exist in the IoT Things layer:

- strength of wireless signals,
- node interception by owner/attackers, and
- nature of network topology.

In addition to this, Replay Attack can easily exploit the confidentiality of this layer by spoofing, altering, or by Timing Attack. Another attack is the Node capture attack which can be made by the attacker by taking over the node and capturing all the information on the node. According to [171] another attack called DoS attack is also possible where the attacker adds another node in the network and threatens the integration of the data. This attack deprives the system of the sleep mode that the nodes normally use to save energy. Cellular networks have started to support new user categories tailored for IoT applications, e.g., narrow band-IoT (NB-IoT). Several challenges arise with the increase in the density of IoT devices. Re-transmission gets more frequent as collision among the IoT devices also increases due to several access requests for IoT devices which affects the energy efficiency. Several approaches are used to aggregate IoT traffic. For instance, in [172] the authors proposed a transmission protocol to aggregate IoT traffic by using drones along with the surety of fair shared spectrum access with the existing cellular users.

B. SECURITY OF IoT-BASED COMMUNICATION

The communication of IoT devices is the target for harmful attacks in the following three classical aspects [173].

- **Confidentiality:** specifies to the communication to be accessed only by authorized persons.
- **Integrity:** refers to the complete trustworthiness transmission and receivable of data without any accidental and intentional modifications.
- **Availability:** is about making sure about the usability of the service upon the authorized request only.

The communication layer is not fully secure and can suffer from the following network attacks (attacks over the network or an attack on the network) [79], [169].

- **Man in the Middle (MITM):** In this attack, the attacker capture, read, and modify data between two objects on the IoT platform [171]. The major goal of the attacker is to change data on the IoT platform by sabotaging the traffic.
- **Spoofing:** In spoofing the attackers imitate or modify the node information to poison the network traffic by generating new nodes, extending or shortening the network paths, or by sending false messages [174], [175]. Spoofing affects the integrity of the IoT system.
- **Desynchronization:** In desynchronization, the attackers interfere with the communication parameters and disturb the normal synchronous network traffic [176], [177].
- **Selective Forwarding:** In selective forwarding, the attacker steals and corrupts the data by seizing the nodes, reducing the number of data packets, and redirecting the packets to different directions in IoT networks.
- **Unfairness:** In unfairness, the attackers distract the equal load sharing of the network, and as a result system gets down.
- **Flooding:** In flooding, the attacker disables a part of the whole IoT network and results in reducing the speed or the complete shut down of the service.

Moreover, the other attacks include wormhole, Sybil, RFID cloning, unauthorized access, sinkhole attacks, denial of service, and routing information attacks, etc.

C. SECURITY OF IoT APPLICATIONS

On the application layer users and machines communicate directly to the IoT platforms. Application layers are not fully secure and face different types of attacks are listed under.

- **Software Attacks:** IoT applications face security vulnerabilities like,
  – Phishing attacks,
  – Virus, worms,
  – Trojan horse,
  – spyware,
  – Malicious scripts and
  – Denial of Service
- **Encryption Attacks:** Along with the software attacks there are encryption attacks that break the system encryption. Some examples are as under:
  – Side channel attacks
  – Crypt-analysis attacks
  – Man in the Middle attack

D. AI-BASED SECURITY APPROACHES

In [178] the authors demonstrated vulnerabilities to different cyberattacks on personal medical device communication. Specifically, how an external attacker can hook into the personal medical device's communication and eavesdrop on the sensitive health data traffic, and implement man-in-the-middle, replay, false data injection, and denial-of-service attacks. The authors proposed an intrusion detection system (IDS), HEKA, for monitoring device traffic and attacks. The proposed system detects irregular traffic-flow patterns using an n-gram based approach and different machine learning techniques for intrusion detection. Undoubtedly, Artificial intelligence (AI) is revolutionizing patient healthcare with its seemingly limitless power. However, the new issues arising from the applications of AI in healthcare can not be ignored. In [179] the authors highlighted the new issues of AI-based applications in healthcare. Big patient data brings big risks about data liability and challenges about patient privacy concerns. In [180], [181] the authors highlighted concerns about cybersecurity, the question of responsibility, and consideration of ethics while integrating AI tools into current practice. In authors [181] addresses four major areas like transparency, informed consent, privacy, and accountability, where guidelines and best practices will be helpful to avoid harmful effects or unwanted consequences. In [182] the authors discussed the uncertain future of AI considering its advantages and disadvantages. AI-based techniques can be used in different fields to achieve excellent results. For instance, according to [183] AI-based robots and machines are replacing laborious and monotonous tasks. AI-based health reports have made doctors work faster and help in providing earlier diagnoses by reducing costs. In [184] the authors highlighted current security solutions with AI i.e., Intrusion Detection and Prevention Systems (IDPS) as well as their limitations and considerations in a power utility network. In [185] the authors presented artificial intelligence analysis benefits in medicine. The authors examined the effect of artificial intelligence assistance in the medical field, the effect of AI-based diagnosis on a patient, patient's treatment (i.e., Precision Medicine), error reduction (i.e., human and machine-based errors), and virtually being present with the patients(i.e., robot nurses, medicine reminders, etc.). In [186] the authors investigated the attack model for IoT systems and IoT security solutions based on machine learning (ML) techniques including supervised learning, unsupervised learning, and reinforcement learning (RL). The main focus was IoT authentication, access control, secure offloading, and malware detection schemes to protect data privacy. In [187] the authors' surveys about the use of AI-based tools for healthcare purposes from consumers' perspectives. According to the author acceptance of AI technology in the healthcare sector requires a deep understanding of the technology and related factors (ethical, regulatory concerns) before its implementation in clinical decision support (CDS).

Based on the identified gaps and the security threats on the three layers of IoT, we aim to develop a system that ensures operational reliability and resilience of personalized and application-specific healthcare services to patients through a coordinated network of IoT applications and devices. In the

TABLE 7. Security threats at different IoT layers [42].

IoT Layers	Attacks	Potential Mitigation
Things	Tampering, Jamming Eavesdropping Denial of Services Physical Attacks Exhaustion	Tamper-resistant packaging Channel surfing , priority messages End-to-end Encryption Spread-spectrum techniques Shared cryptography Keys or routing tables Rate limitation
Communication	MITM, Spoofing Desynchronization Selective forwarding Unfairness, Wormhole, Sybil Flooding	Security monitoring token-based authorization Semantic network firewall Traffic control, Link Authentication Client puzzles
Application	Phishing attacks Virus, worms, Trojan horse spyware, Malicious scripts Denial of Services Side channel attacks Crypt-analysis, MITM Trojan	Security training antivirus Traceability Validation

following section, we discussed various components and workflow of our proposed solution.

VII. PROPOSED SOLUTION

To ensure the operational reliability of coordinated healthcare IoT devices and applications to deliver personalized healthcare services, we plan to develop a methodology that includes the following three components:

- **Modeling:** To investigate various modeling techniques that help to develop an abstract but practical model of operational characteristics of IoT devices, applications, healthcare conditions, and standards.
- **Reliability Analysis:** Based on the developed model, investigate various techniques to analyze the following questions:
  - How to establish reliable coordination among applications and devices?
  - How to diagnose the right cause of the health condition?
  - How to identify the right treatment that minimizes its side-effects on other health conditions?
- **Resilience Analysis:** To investigate techniques that ensure fail-safe operations of the devices and applications through continuous health monitoring.

A. WORKFLOW OF CPHS

The Workflow of the personalized HIoT System for comprehensive personalized healthcare is shown in Figure 14. Patient data from different monitoring devices like an insulin pump, blood pressure monitor, blood cholesterol monitor, and heart rate monitor is collected and transmitted at the IoT cloud where data is stored. Stored data is processed by using different AI techniques and disease models. However, several challenges are involved to develop the personalized HIoT System for comprehensive personalized healthcare.

To address these challenges, we aim to develop a solution that enables the modeling of health conditions based on their clinical/biological characteristics including clinical/biological dependencies among the conditions. Based on the models, we develop a personalized healthcare monitor that monitors various health conditions of a patient, and identifies any discrepancies among health conditions. Furthermore, the monitor provides clinical reasoning to rigorously identify the exact cause of the discrepancy. Once identified, the monitor can provide corresponding treatment to the discrepancy which can be later monitored to understand the effect of the treatment. Based on clinical reasoning, the monitor controls various health conditions of a patient remotely and automatically. Clinical reasoning makes the monitor self-aware, (i.e., it understands what it is monitoring), and thus supports healthcare services that are free of false diagnosis. Modeling health conditions is a challenging task as it requires identifying different clinical dependencies among various health conditions of a patient. However, these dependencies are typically non-trivial that require understanding of the underlying variable level biological processes associated with the conditions which are mostly a black box. To describe different levels of details about biological processes, we will introduce a modeling language that will allow modeling health conditions and their dependencies at an abstract but practical level of description. The model will be later used for mechanized reasoning about dependencies among the health conditions.

B. FEATURES OF CPHS

Our proposed methodology will not only realize personalized healthcare services based on their clinical characteristics but will also enable autonomous, automatic, and rigorous diagnosis of stealthy health conditions exploiting biological dependencies among various health conditions. Of course, we will address the key challenge to model clinical

TABLE 8. Comparison of various smart healthcare approaches.

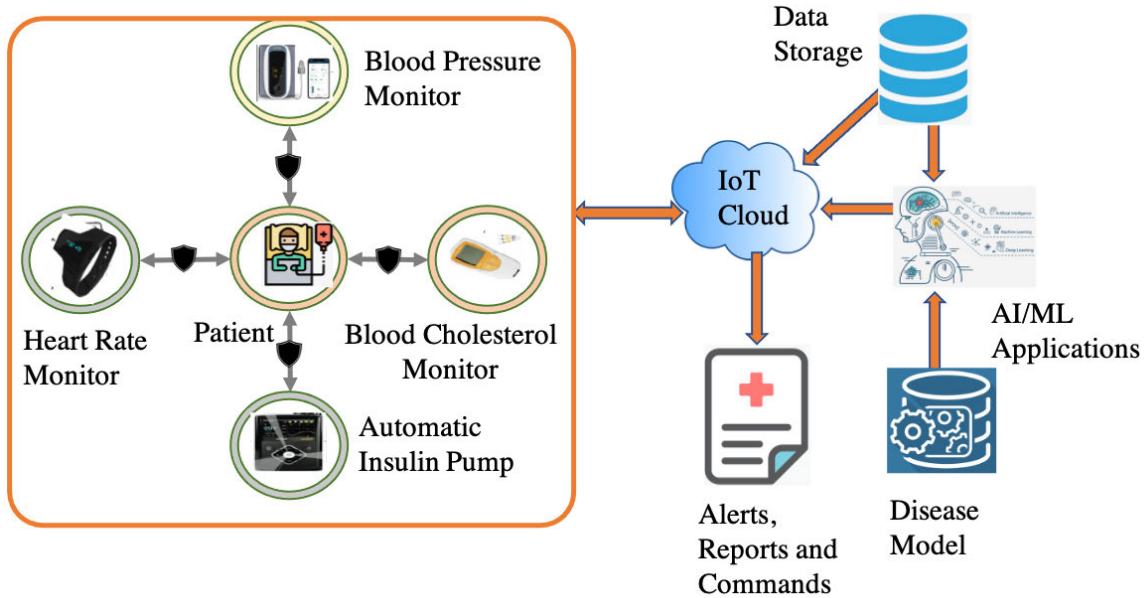| Healthcare Services	Reliability	Resilience	Personalization (of individual health condition)	Personalization (of multiple health conditions)
Smart healthcare [63], [75], [78], [79], [81]–[84]	◐	◐	◐	○
AI-based [7], [96], [134]	◐	◐	◐	○
ML/DL-based [27], [117]	◐	◐	◐	○
CPHS (this work)	●	●	●	●

FIGURE 14. Workflow of personalised HIoT.

characteristics of health conditions that are highly declarative and abstract (e.g., health conditions with no specific clinical characteristics) on one hand, but are very low level (e.g., DNA and other details of a health condition) on the other hand. We aim to demonstrate the effectiveness of our methodology through its application to observe various health conditions (e.g., heart rate, diabetes, blood pressure, and cholesterol-related).

Consequently, we will develop a library of various health conditions (models) that can be later used in any healthcare computerized system to reason about healthcare services based on their clinical characteristics. The library will also help to learn other dependencies among various health conditions that are otherwise beyond the capabilities of medical practitioners. Moreover, based on the models, the newly identified dependencies will be explainable in a way that is understood by practitioners and machine.

Based on our results, we aim to integrate our method with following technologies:

- Blockchain-based techniques to obtain integrity and reliability for personalized healthcare services.

- AI/ML techniques that will help to better understand health conditions by comparing data of different patients for similar health conditions and consequently proposing more personalized diagnosis and treatment, that will effectively and efficiently improve the health of patients.

As personalized healthcare and AI are evolving continuously, comprehensive biological knowledge, smart diagnostic techniques, and other factors like patient data from the medical images, and patient history will help to identify personalized therapies for individuals. AI is playing a vital role in different fields of healthcare. So far AI is used at Things, Communication, and Navigation layers for data collection, communication, and patient monitoring respectively. However, AI is not yet completely safe for diagnosis and treatment purposes due to its explainability and trust issues. Therefore, AI algorithms are not yet fully trusted in critical healthcare domains.

VIII. CONCLUSION

We have introduced Healthcare 5.0, personalized healthcare services, and their key requirements that are classified into reliability, resilience, and personalized healthcare. Importantly, we have defined personalized healthcare services as

a relationship of various health conditions of a patient based on the characteristics of their underlying biological process as well as their associated mechanical monitoring system. Based on the reference architecture of a modern IoT-based healthcare system, we have investigated the current efforts to address the defined key requirements. Finally, we have identified research gaps that need to be addressed to develop reliable and resilient personalized healthcare systems for the future.

REFERENCES

[1] T.S.U.A. 2030. (Sep. 2015). *Transforming Our World: The 2030 Agenda for Sustainable Development*. [Online]. Available: https://sdgs.un.org/2030agenda

[2] D. Sherman. (Nov. 2017). *Health 5.0: The Emergence of Digital Wellness*. [Online]. Available: https://medium.com/qut-cde/health-5-0-the-emergence-of-digital-wellness-b21fdff635b9

[3] E. Bercovich and M. C. Javitt, "Medical imaging: From roentgen to the digital revolution, and beyond," *Rambam Maimonides Med. J.*, vol. 9, no. 4, p. e0034, Oct. 2018.

[4] A. Giri, S. Dutta, S. Neogy, K. Dahal, and Z. Pervez, "Internet of Things (IoT): A survey on architecture, enabling technologies, applications and challenges," in *Proc. 1st Int. Conf. Internet Things Mach. Learn.*, New York, NY, USA, Oct. 2017, pp. 1–12, doi: 10.1145/3109761.3109768.

[5] G. V. Research. (Mar. 2019). *Healthcare Market Trends*. [Online]. Available: https://www.reportlinker.com/p05763769/Internet-of-Things-in-Healthcare-Market-Size-Share-Trends-Analysis-Report-By-Component-By-Connectivity-Technology-By-End-Use-By-Application-And-Segment-Forecasts.html

[6] S. J. Ramson, S. Vishnu, and M. Shanmugam, "Applications of Internet of Things (IoT)–An overview," in *Proc. 5th Int. Conf. Devices, Circuits Syst. (ICDCS)*, Mar. 2020, pp. 92–95.

[7] K. Zhan, "Sports and health big data system based on 5G network and Internet of Things system," *Microprocessors Microsyst.*, vol. 80, Feb. 2021, Art. no. 103363.

[8] O. AlShorman, B. AlShorman, M. Alkhassaweneh, and F. Alkahtani, "A review of internet of medical things (IoMT)–based remote health monitoring through wearable sensors: A case study for diabetic patients," *Indonesian J. Elect. Eng. Comput. Sci.*, vol. 20, no. 1, pp. 414–422, 2020.

[9] *IEEE Standard Glossary of Software Engineering Terminology*, IEEE Standard 610.12-1990, 1990, pp. 1–84.

[10] S. Vyas, M. Gupta, and R. Yadav, "Converging blockchain and machine learning for healthcare," in *Proc. Amity Int. Conf. Artif. Intell. (AICAI)*, Feb. 2019, pp. 709–711.

[11] A. Vergutz, G. Noubir, and M. Nogueira, "Reliability for smart healthcare: A network slicing perspective," *IEEE Netw.*, vol. 34, no. 4, pp. 91–97, Jul. 2020.

[12] E. Zaitseva, V. Levashenko, M. Kvassay, and T. M. Deserno, "Reliability estimation of healthcare systems using fuzzy decision trees," in *Proc. Ann. Comput. Sci. Inf. Syst.*, Oct. 2016, pp. 331–340.

[13] D. Firesmith. *System Resilience: What Exactly is it?* Accessed: Nov. 2019. [Online]. Available: http://insights.sei.cmu.edu/blog/system-resilience-what-exactly-is-it/

[14] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Depend. Sec. Comput.*, vol. 1, no. 1, pp. 11–33, Jan./Mar. 2004.

[15] J. Zhang, L. Li, G. Lin, D. Fang, Y. Tai, and J. Huang, "Cyber resilience in healthcare digital twin on lung cancer," *IEEE Access*, vol. 8, pp. 201900–201913, 2020.

[16] J. Rajamaki, J. Nevmerzhitskaya, and C. Virag, "Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF)," in *Proc. IEEE Global Eng. Educ. Conf. (EDUCON)*, Apr. 2018, pp. 2042–2046.

[17] A. Sood and K. Moidu, "Protection of healthcare information: Adding cyber resilience and recovery," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2018, pp. 132–134.

[18] S. Safavi, A. M. Meer, E. Keneth Joel Melanie, and Z. Shukur, "Cyber vulnerabilities on smart healthcare, review and solutions," in *Proc. Cyber Resilience Conf. (CRC)*, Nov. 2018, pp. 1–5.

[19] S. Zhang, S. M. H. Bamakan, Q. Qu, and S. Li, "Learning for personalized medicine: A comprehensive review from a deep learning perspective," *IEEE Rev. Biomed. Eng.*, vol. 12, pp. 194–208, 2019.

[20] L. A. Chauveau, N. Szilas, A. L. Luiu, and F. Ehrler, "Dimensions of personalization in a narrative pedagogical simulation for Alzheimer's caregivers," in *Proc. IEEE 6th Int. Conf. Serious Games Appl. Health (SeGAH)*, May 2018, pp. 1–8.

[21] K. Zimmer. (Mar. 2021). *The Ultimate Incubator: The Brave New World of Bionic Babies*. [Online]. Available: https://spectrum.ieee.org/biomedical/devices/the-ultimate-incubator-the-brave-new-world-of-bionic-babies

[22] M. Pollind, R. Soangra, M. Grant-Beuttler, and A. Aminian. (Apr. 2019). *Customized Wearable Sensor-Based Insoles for Gait Re-Training in Idiopathic Toe Walkers*. [Online]. Available: https://diatribe.org/understanding-insulin-pump-settings

[23] F. Velcani and K. Yan. (Jan. 2021). *Understanding Insulin Pump Settings*. [Online]. Available: https://diatribe.org/understanding-insulin-pump-settings

[24] A. Almogbil, A. Alghofaili, C. Deane, and T. Leschke, "Digital forensic analysis of fitbit wearable technology: An investigator's guide," in *Proc. 7th IEEE Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)/6th IEEE Int. Conf. Edge Comput. Scalable Cloud (EdgeCom)*, Aug. 2020, pp. 44–49.

[25] E. V. Karpova, E. E. Karyakina, and A. A. Karyakin, "Wearable non-invasive monitors of diabetes and hypoxia through continuous analysis of sweat," *Talanta*, vol. 215, Aug. 2020, Art. no. 120922. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0039914020302137

[26] X. Weng and S. Neethirajan, "Immunosensor based on antibody-functionalized MoS_2 for rapid detection of avian coronavirus on cotton thread," *IEEE Sensors J.*, vol. 18, no. 11, pp. 4358–4363, Jun. 2018.

[27] B. He, K. Shu, and H. Zhang, "Diabetes diagnosis and treatment research based on machine learning," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Aug. 2019, pp. 675–679.

[28] C. Berget, S. Lange, L. Messer, and G. P. Forlenza, "A clinical review of the T: Slim X2 insulin pump," *Expert Opinion Drug Del.*, vol. 17, no. 12, pp. 1675–1687, 2020.

[29] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering–A systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, 2009.

[30] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Keele Univ., Durham Univ. Joint Rep., Tech. Rep. EBSE 2007-001, 2007. [Online]. Available: http://www.dur.ac.uk/ebse/resources/Systematic-reviews-5-8.pdf

[31] C. Okoli and K. Schabram, "A guide to conducting a systematic literature review of information systems research," Concordia Univ., Montreal, QC, Canada, Tech. Rep., 2010. [Online]. Available: http://sprouts.aisnet.org/10-26

[32] A. Dridi, S. Sassi, and S. Faiz, "A smart IoT platform for personalized healthcare monitoring using semantic technologies," in *Proc. IEEE 29th Int. Conf. Tools with Artif. Intell. (ICTAI)*, Boston, MA, USA, Nov. 2017, pp. 1198–1203, doi: 10.1109/ICTAI.2017.00182.

[33] P. Amin, N. R. Anikireddypally, S. Khurana, S. Vadakkemadathil, and W. Wu, "Personalized health monitoring using predictive analytics," in *Proc. IEEE 5th Int. Conf. Big Data Comput. Service Appl. (BigDataService)*, Apr. 2019, pp. 271–278.

[34] G. Alfian, M. Syafrudin, M. Ijaz, M. Syaekhoni, N. Fitriyani, and J. Rhee, "A personalized healthcare monitoring system for diabetic patients by utilizing BLE-based sensors and real-time data processing," *Sensors*, vol. 18, no. 7, p. 2183, Jul. 2018, doi: 10.3390/s18072183.

[35] A. R. Khushk and X. Li, "Petri net methodology for solving healthcare management issues," in *Proc. ITM Web Conf.*, vol. 17, 2018, Art. no. 03030, doi: 10.1051/itmconf/20181703030.

[36] M. U. Ahmed, "A personalized health-monitoring system for elderly by combining rules and case-based reasoning," *Stud. Health Technol. Informat.*, vol. 211, pp. 249–254, Mar. 2015. [Online]. Available: http://europepmc.org/abstract/MED/25980877

[37] R. Ali, M. Afzal, M. Hussain, M. Ali, M. H. Siddiqi, S. Lee, and B. Ho Kang, "Multimodal hybrid reasoning methodology for personalized wellbeing services," *Comput. Biol. Med.*, vol. 69, pp. 10–28, Feb. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0010482515003819

[38] M. Ma, M. Skubic, K. Ai, and J. Hubbard, "Angel-echo: A personalized health care application," in *Proc. IEEE/ACM Int. Conf. Connected Health: Appl., Syst. Eng. Technol. (CHASE)*, Jul. 2017, pp. 258–259.

[39] C. Chen, E.-W. Loh, K. Kuo, and K.-W. Tam, "The times they are a-Changin'–healthcare 4.0 is coming!" *J. Med. Syst.*, vol. 44, p. 40, Dec. 2019.

[40] B. Wolf and C. Scholze, "'Omedicine 4.0,'" *Current Directions Biomed. Eng.*, vol. 3, pp. 183–186, Sep. 2017.

[41] C. Yan, G. Duan, Y. Zhang, F.-X. Wu, Y. Pan, and J. Wang, "Predicting drug-drug interactions based on integrated similarity and semi-supervised learning," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, early access, Apr. 16, 2020, doi: 10.1109/TCBB.2020.2988018.

[42] D. Singh, P. Pal, M. Mishra, A. Lamba, and S. Swagatika, "Security issues in different layers of IoT and their possible mitigation," *Int. J. Sci. Technol. Res.*, vol. 9, no. 4, pp. 2762–2771, May 2020, doi: 10.13140/RG.2.2.32754.04803.

[43] S. Nasiri, F. Sadoughi, M. H. Tadayon, and A. Dehnad, "Security requirements of Internet of Things-based healthcare system: A survey study," *Acta Inform. Medica*, vol. 27, no. 4, pp. 253–258, Dec. 2019. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7004290/pdf/AIM-27-253.pdf

[44] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, "The future of healthcare Internet of Things: A survey of emerging technologies," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1121–1167, 2nd Quart., 2020.

[45] Y. Li, Y. Li, N. Wang, and H. Wang, "A Petri net based model for a cloud healthcare system," in *Proc. Chin. Control Decis. Conf. (CCDC)*, Jun. 2018, pp. 3928–3931.

[46] K. W. Ching and M. M. Singh, "Wearable technology devices security and privacy vulnerability analysis," *Int. J. Netw. Secur. Appl.*, vol. 8, no. 3, pp. 19–30, May 2016.

[47] M. Hooshmand, D. Zordan, D. D. Testa, E. Grisan, and M. Rossi, "Boosting the battery life of wearables for health monitoring through the compression of biosignals," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1647–1662, Oct. 2017.

[48] Y. Yin, Y. Zeng, X. Chen, and Y. Fan, "The Internet of Things in healthcare: An overview," *J. Ind. Inf. Integr.*, vol. 1, pp. 3–13, Mar. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2452414X16000066

[49] L. C. Clark, Jr., and C. Lyons, "Electrode systems for continuous monitoring in cardiovascular surgery," *Ann. New York Acad. Sci.*, vol. 102, no. 1, pp. 29–45, 1962.

[50] D. Dhankhar, R. Li, A. Nagpal, J. Chen, T. C. Cesario, and P. M. Rentzepis, "Extending human vision to infrared and ultraviolet light: A study using micro-particles and fluorescent molecules," *IEEE Access*, vol. 8, pp. 73890–73897, 2020.

[51] J.-Z. Sun, G. Peter Kingori, R.-W. Si, D.-D. Zhai, Z.-H. Liao, D.-Z. Sun, T. Zheng, and Y.-C. Yong, "Microbial fuel cell-based biosensors for environmental monitoring: A review," *Water Sci. Technol.*, vol. 71, no. 6, pp. 801–809, Mar. 2015.

[52] J. Wang, M. Tanaka, and M. Okochi, "Quartz crystal microbalance sensor based on peptide anchored single-walled carbon nanotubes for highly selective TNT explosive detection," in *Proc. IEEE SENSORS*, Oct. 2020, pp. 1–3.

[53] F. F. Franco, L. Manjakkal, and R. Dahiya, "Screen-printed flexible carbon versus silver electrodes for electrochemical sensors," in *Proc. IEEE Int. Conf. Flexible Printable Sensors Syst. (FLEPS)*, Aug. 2020, pp. 1–4.

[54] A. K. Singh and S. K. Jha, "Fabrication and validation of a handheld non-invasive, optical biosensor for self-monitoring of glucose using saliva," *IEEE Sensors J.*, vol. 19, no. 18, pp. 8332–8339, Sep. 2019.

[55] N. P. Revsbech, M. Nielsen, and D. Fapyane, "Ion selective amperometric biosensors for environmental analysis of nitrate, nitrite and sulfate," *Sensors*, vol. 20, no. 15, p. 4326, Aug. 2020.

[56] M. Fani, M. Rezayi, Z. Meshkat, S. A. Rezaee, M. Makvandi, and K. Ahmadi Angali, "A novel electrochemical DNA biosensor based on a gold nanoparticles-reduced graphene oxide-polypyrrole nanocomposite to detect human T-lymphotropic virus-1," *IEEE Sensors J.*, vol. 20, no. 18, pp. 10625–10632, Sep. 2020.

[57] B. Rawat, K. K. Mishra, U. Barman, L. Arora, D. Pal, and R. P. Paily, "Two-dimensional MoS_2-based electrochemical biosensor for highly selective detection of glutathione," *IEEE Sensors J.*, vol. 20, no. 13, pp. 6937–6944, Jul. 2020.

[58] J. Malik, S. K. Oruganti, D. Paul, and F. Bien, "Fully implantable miniature RF sensor for continuous glucose monitoring system," in *Proc. IEEE Int. Symp. Radio-Freq. Integr. Technol. (RFIT)*, Aug. 2019, pp. 1–2.

[59] S. Kumar, R. Singh, B. K. Kaushik, N. Chen, Q. S. Yang, and X. Zhang, "LSPR-based cholesterol biosensor using hollow core fiber structure," *IEEE Sensors J.*, vol. 19, no. 17, pp. 7399–7406, Sep. 2019.

[60] S. Schroder, H. K. Gatty, G. Stemme, N. Roxhed, and F. Niklaus, "A low-cost nitric oxide gas sensor based on bonded gold wires," in *Proc. 19th Int. Conf. Solid-State Sensors, Actuat. Microsyst. (TRANSDUCERS)*, Jun. 2017, pp. 1457–1460.

[61] J. Yang, Y. Cao, and N. Zhang, "Spectrophotometric method for superoxide anion radical detection in a visible light (400–780 nm) system," *Spectrochim. Acta A, Mol. Biomol. Spectroscopy*, vol. 239, Oct. 2020, Art. no. 118556.

[62] S. Pokorni, "Reliability and availability of the Internet of Things," *Mil. Tech. Courier*, vol. 67, p. 588, Jun. 2019.

[63] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things security: A top-down survey," *Comput. Netw.*, vol. 141, pp. 199–221, Aug. 2018.

[64] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[65] A. Rayes and S. Salam, *Internet of Things From Hype to Reality*. Cham, Switzerland: Springer, 2017.

[66] M. Kim, "A qualitang model for evaluating IoT applications," *Int. J. Comput. Electr. Eng.*, vol. 8, no. 1, p. 66, 2016.

[67] A. Karkouch, H. Mousannif, H. Al Moatassime, and T. Noel, "Data quality in Internet of Things: A state-of-the-art survey," *J. Netw. Comput. Appl.*, vol. 73, pp. 57–81, Sep. 2016.

[68] M. R. Valanarasu, "Smart and secure IoT and AI integration framework for hospital environment," *J. ISMAC*, vol. 1, no. 3, pp. 172–179, 2019.

[69] M. M. Alam, H. Malik, M. I. Khan, T. Pardy, A. Kuusik, and Y. L. Moullec, "A survey on the roles of communication technologies in IoT-based personalized healthcare applications," *IEEE Access*, vol. 6, pp. 36611–36631, 2018.

[70] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[71] A. Choudhury and D. Gupta, "A survey on medical diagnosis of diabetes using machine learning techniques," in *Recent Developments in Machine Learning and Data Analytics*. Singapore: Springer, 2019, pp. 67–78.

[72] D.-N. Le, B. Seth, and S. Dalal, "A hybrid approach of secret sharingwith fragmentation and encryptionin cloud environment for SecuringOutsourced medical database: A revolutionary approach," *J. Cyber Secur. Mobility*, vol. 7, no. 4, pp. 379–408, 2018.

[73] T. Alam, "A reliable framework for communication in internet of smart devices using IEEE 802.15. 4," *ARPN J. Eng. Appl. Sci.*, vol. 13, no. 10, pp. 1–10, Oct. 2018.

[74] A. Lay-Ekuakille, N. I. Giannoccaro, P. Vergallo, E. Greco, and G. Griffo, "Smartness for railway transducers: Reliability experimental verifications and accuracy," *IEEE Sensors J.*, vol. 15, no. 5, pp. 2614–2621, May 2015.

[75] M. innovation briefing. (Feb. 2016). *Medtronic*. [Online]. Available: https://www.medtronic-diabetes.co.U.K./sites/U.K./medtronic-diabetes.co.U.K./files/minimed640gifu2015mp6025957-024_a_en_mmol.compressed.pdf

[76] Z. Lv, L. Qiao, J. Li, and H. Song, "Deep-learning-enabled security issues in the Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9531–9538, Jun. 2021.

[77] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Internet of Things: Evolution and technologies from a security perspective," *Sustain. Cities Soc.*, vol. 54, Mar. 2020, Art. no. 101728.

[78] R. Lopez Leal, A. G. Martinez Lopez, A. L. Herrera May, and J. Martinez Castillo, "Reliability analysis sensors based on embedded system," in *Proc. Int. Conf. Comput. Syst. Telematics (ICCSAT)*, Oct. 2015, pp. 1–5.

[79] J. Yang, S. He, Y. Lin, and Z. Lv, "Multimedia cloud transmission and storage system based on Internet of Things," *Multimedia Tools Appl.*, vol. 76, no. 17, pp. 17735–17750, Sep. 2017.

[80] J. Rajamäki, "Towards a design theory for resilient (sociotech-nical, cyber-physical, software-intensive and systems of) systems," Laurea Univ. Appl. Sci., Tech. Rep., 2016. [Online]. Available: https://urn.fi/URN:ISBN:978-1-61804-365-8

[81] K. Khalil, O. Eldash, A. Kumar, and M. Bayoumi, "Machine learning-based approach for hardware faults prediction," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 11, pp. 3880–3892, Nov. 2020.

[82] M. Letafati, A. Kuhestani, K. K. Wong, and M. J. Piran, "A lightweight secure and resilient transmission scheme for the Internet of Things in the presence of a hostile jammer," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4373–4388, Mar. 2021.

[83] Y. Sharma, B. Javadi, W. Si, and D. Sun, "Reliability and energy efficiency in cloud computing systems: Survey and taxonomy," *J. Netw. Comput. Appl.*, vol. 74, pp. 66–85, Oct. 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804516301746

[84] M. Yanovsky, O. Yanovskaya, and V. Kharchenko, "Analysis of methods for providing availability and accessibility of cloud services," in *ICT in Education, Research and Industrial Applications*. Kyiv, Ukraine: CEUR-WS, 2016, pp. 414–426.

[85] A. Strielkina, V. Kharchenko, and D. Uzun, "Availability models for healthcare IoT systems: Classification and research considering attacks on vulnerabilities," in *Proc. IEEE 9th Int. Conf. Dependable Syst., Services Technol. (DESSERT)*, May 2018, pp. 58–62.

[86] C. Tsigkanos, S. Nastic, and S. Dustdar, "Towards resilient Internet of Things: Vision, challenges, and research roadmap," in *Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2019, pp. 1754–1764.

[87] S. M. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[88] P. A. Laplante, M. Kassab, N. L. Laplante, and J. M. Voas, "Building caring healthcare systems in the Internet of Things," *IEEE Syst. J.*, vol. 12, no. 3, pp. 3030–3037, Sep. 2018.

[89] V. Kharchenko, M. Kolisnyk, I. Piskachova, and N. Bardis, "Reliability and security issues for IoT-based smart business center: Architecture and Markov model," in *Proc. 3rd Int. Conf. Math. Comput. Sci. Ind. (MCSI)*, Aug. 2016, pp. 313–318.

[90] A. Strielkina, D. Uzun, and V. Kharchenko, "Modelling of healthcare IoT using the queueing theory," in *Proc. 9th IEEE Int. Conf. Intell. Data Acquisition Adv. Comput. Syst., Technol. Appl. (IDAACS)*, Sep. 2017, pp. 849–852.

[91] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. Rodrigues, and Y. Park, "BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment," *IEEE Access*, vol. 8, pp. 95956–95977, 2020.

[92] S. Khan and M. Alam, "Wearable Internet of Things for personalized healthcare: Study of trends and latent research," in *Health Informatics: A Computational Perspective in Healthcare*. Singapore: Springer, 2021.

[93] S. K. Datta, C. Bonnet, A. Gyrard, R. Costa, and K. Boudaoud, "Applying Internet of Things for personalized healthcare in smart Homes," *10 2015*, pp. 164–169.

[94] L.-J. Kau and C.-S. Chen, "A smart phone-based pocket fall accident detection, positioning, and rescue system," *IEEE J. Biomed. Health Inform.*, vol. 19, no. 1, pp. 44–56, Jan. 2015.

[95] Z. Zhang, T. He, M. Zhu, Q. Shi, and C. Lee, "Smart triboelectric socks for enabling artificial intelligence of things (AIoT) based smart home and healthcare," in *Proc. IEEE 33rd Int. Conf. Micro Electro Mech. Syst. (MEMS)*, Jan. 2020, pp. 80–83.

[96] A. Haleem, M. Javaid, R. P. Singh, and R. Suman, "Applications of artificial intelligence (AI) for cardiology during COVID-19 pandemic," *Sustain. Oper. Comput.*, vol. 2, pp. 71–78, Nov. 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666412721000155

[97] V. Jagadeeswari, V. Subramaniyaswamy, R. Logesh, and V. Vijayakumar, "A study on medical Internet of Things and big data in personalized healthcare system," *Health Inf. Sci. Syst.*, vol. 6, no. 1, pp. 1–20, Dec. 2018.

[98] K. S. Mohamed, *IoT Networking and Communication Layer*. Cham, Switzerland: Springer, 2019, pp. 49–70, doi: 10.1007/978-3-030-18133-8_3.

[99] M. Aydos, Y. Vural, and A. Tekerek, "Assessing risks and threats with layered approach to Internet of Things security," *Meas. Control*, vol. 52, Apr. 2019, Art. no. 002029401983799.

[100] S. J. Moore, C. D. Nugent, S. Zhang, and I. Cleland, "IoT reliability: A review leading to 5 key research directions," *CCF Trans. Pervasive Comput. Interact.*, vol. 2, no. 3, pp. 147–163, Oct. 2020.

[101] E. Al-Masri, "QoS-aware IIoT microservices architecture," in *Proc. IEEE Int. Conf. Ind. Internet (ICII)*, Oct. 2018, pp. 171–172.

[102] S. Li and J. Huang, "GSPN-based reliability-aware performance evaluation of IoT services," in *Proc. IEEE Int. Conf. Services Comput. (SCC)*, Jun. 2017, pp. 483–486.

[103] S. Sinche, O. Polo, D. Raposo, M. Femandes, F. Boavida, A. Rodrigues, V. Pereira, and J. Sa Silva, "Assessing redundancy models for IoT reliability," in *Proc. IEEE 19th Int. Symp. 'World Wireless, Mobile Multimedia Netw.' (WoWMoM)*, Jun. 2018, pp. 14–15.

[104] C. Kamyod, "End-to-end reliability analysis of an IoT based smart agriculture," in *Proc. Int. Conf. Digital Arts, Media Technol. (ICDAMT)*, Feb. 2018, pp. 258–261.

[105] A. Brogi and S. Forti, "QoS-aware deployment of IoT applications through the fog," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1185–1192, Oct. 2017.

[106] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, "Fog computing for healthcare 4.0 environment: Opportunities and challenges," *Comput. Elect. Eng.*, vol. 72, pp. 1–13, Nov. 2018.

[107] P. Tuset-Peiro, F. Adelantado, X. Vilajosana, and R. D. Gomes, "Reliability through modulation diversity: Can combining multiple IEEE 802.15.4-2015 SUN modulations improve PDR?" in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2020, pp. 1–6.

[108] A. Akbar, M. Ibrar, M. A. Jan, A. K. Bashir, and L. Wang, "SDN-enabled adaptive and reliable communication in IoT-fog environment using machine learning and multiobjective optimization," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3057–3065, Nov. 2021.

[109] M. Humayun, N. Jhanjhi, M. Alruwaili, S. S. Amalathas, V. Balasubramanian, and B. Selvaraj, "Privacy protection and energy optimization for 5G-aided industrial Internet of Things," *IEEE Access*, vol. 8, pp. 183665–183677, 2020.

[110] A. Ahad, M. Tahir, and K.-L.-A. Yau, "5G-based smart healthcare network: Architecture, taxonomy, challenges and future research directions," *IEEE Access*, vol. 7, pp. 100747–100762, 2019.

[111] H. Kim, E. A. Lee, and S. Dustdar, "Creating a resilient IoT with edge computing," *Computer*, vol. 52, no. 8, pp. 43–53, Aug. 2019.

[112] K. E. Benson, G. Wang, N. Venkatasubramanian, and Y.-J. Kim, "Ride: A resilient IoT data exchange middleware leveraging SDN and edge cloud resources," in *Proc. IEEE/ACM 3rd Int. Conf. Internet–Things Design Implement. (IoTDI)*, Apr. 2018, pp. 72–83.

[113] D. O'Keeffe, T. Salonidis, and P. Pietzuch, "Frontier: Resilient edge processing for the Internet of Things," *Proc. VLDB Endowment*, vol. 11, no. 10, pp. 1178–1191, Jun. 2018.

[114] K. E. Benson, Q. Han, K. Kim, P. Nguyen, and N. Venkatasubramanian, "Resilient overlays for IoT-based community infrastructure communications," in *Proc. IEEE 1st Int. Conf. Internet–Things Design Implement. (IoTDI)*, Apr. 2016, pp. 152–163.

[115] D. P. Abreu, K. Velasquez, M. Curado, and E. Monteiro, "A resilient Internet of Things architecture for smart cities," *Ann. Telecommun.*, vol. 72, nos. 1–2, pp. 19–30, Feb. 2017.

[116] M. Babar, M. U. Tariq, and M. A. Jan, "Secure and resilient demand side management engine using machine learning for IoT-enabled smart grid," *Sustain. Cities Soc.*, vol. 62, Nov. 2020, Art. no. 102370. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2210670720305904

[117] W. Zeng and J. Zhang, "Leakage-resilient and lightweight authenticated key exchange for E-health," in *Proc. 6th Int. Conf. Inf. Manage. (ICIM)*, Mar. 2020, pp. 162–166.

[118] G. Gardašević, K. Katzis, D. Bajić, and L. Berbakov, "Emerging wireless sensor networks and Internet of Things technologies—Foundations of smart healthcare," *Sensors*, vol. 20, no. 13, p. 3619, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/13/3619

[119] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. K. Al-Ali, and R. Jain, "Recent advances in the internet-of-medical-things (IoMT) systems security," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8707–8718, Jun. 2021.

[120] M. Hariram, S. Banshilal, S. Najeerabanu, and V. Yasuvanth, "Observational study of WPAN and LPWA technologies for various IoT devices and its applications," *Int. J. Adv. Sci. Technol.*, vol. 29, no. 5, pp. 4231–4243, May 2020.

[121] Y. Li, H. Wang, Y. Li, and L. Li, "Patient assignment scheduling in a cloud healthcare system based on Petri net and greedy-based heuristic," *Enterprise Inf. Syst.*, vol. 13, no. 4, pp. 515–533, 2019, doi: 10.1080/17517575.2018.1526323.

[122] S. Jovanović, M. Jovanović, T. Škorić, S. Jokić, B. Milovanović, K. Katzis, and D. Bajić, "A mobile crowd sensing application for hypertensive patients," *Sensors*, vol. 19, no. 2, p. 400, Jan. 2019.

[123] H. Fouad, A. S. Hassanein, A. M. Soliman, and H. Al-Feel, "Analyzing patient health information based on IoT sensor with AI for improving patient assistance in the future direction," *Measurement*, vol. 159, Jul. 2020, Art. no. 107757. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0263224120302955

[124] J. Hathaliya, P. Sharma, S. Tanwar, and R. Gupta, "Blockchain-based remote patient monitoring in healthcare 4.0," in *Proc. IEEE 9th Int. Conf. Adv. Comput. (IACC)*, Dec. 2019, pp. 87–91.

[125] S. U. Amin and M. S. Hossain, "Edge intelligence and Internet of Things in healthcare: A survey," *IEEE Access*, vol. 9, pp. 45–59, 2021.

[126] A. Väänänen, K. Haataja, and P. Toivanen, "Survey to healthcare professionals on the practicality of AI services for healthcare," *FResearch*, vol. 9, p. 760, Jul. 2020.

[127] F. Corno, L. De Russis, and A. M. Roffarello, "A healthcare support system for assisted living facilities: An IoT solution," in *Proc. IEEE 40th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jun. 2016, pp. 344–352.

[128] L. Y. Mano, B. S. Faiçal, L. H. V. Nakamura, P. H. Gomes, G. L. Libralon, R. I. Meneguete, G. P. R. Filho, G. T. Giancristofaro, G. Pessin, B. Krishnamachari, and J. Ueyama, "Exploiting IoT technologies for enhancing health smart Homes through patient identification and emotion recognition," *Comput. Commun.*, vols. 89–90, pp. 178–190, Sep. 2016.

[129] J. Kaur and K. S. Mann, "AI based healthcare platform for real time, predictive and prescriptive analytics using reactive programming," in *Proc. J. Phys., Conf.*, 2017, vol. 933, no. 1, Art. no. 012010.

[130] A. J. Jara, M. A. Zamora-Izquierdo, and A. F. Skarmeta, "Interconnection framework for mHealth and remote monitoring based on the Internet of Things," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 47–65, Sep. 2013.

[131] G. Gardašević, K. Katzis, D. Bajić, and L. Berbakov, "Emerging wireless sensor networks and Internet of Things technologies—Foundations of smart healthcare," *Sensors*, vol. 20, no. 13, p. 3619, 2020.

[132] A. Esteva, B. Kuprel, R. A. Novoa, J. Ko, S. M. Swetter, H. M. Blau, and S. Thrun, "Dermatologist-level classification of skin cancer with deep neural networks," *Nature*, vol. 542, no. 7639, pp. 115–118, 2017.

[133] F. Ali, S. El-Sappagh, S. M. R. Islam, D. Kwak, A. Ali, M. Imran, and K.-S. Kwak, "A smart healthcare monitoring system for heart disease prediction based on ensemble deep learning and feature fusion," *Inf. Fusion*, vol. 63, pp. 208–222, Nov. 2020.

[134] E. B. Sloane and R. J. Silva, "Artificial intelligence in medical devices and clinical decision support systems," in *Clinical Engineering Handbook*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 556–568.

[135] P. Marcelis, N. Kouvelas, V. S. Rao, and V. Prasad, "DaRe: Data recovery through application layer coding for LoRaWAN," *IEEE Trans. Mobile Comput.*, early access, Aug. 14, 2020, doi: 10.1109/TMC.2020.3016654.

[136] P. Pronovost, S. Berenholtz, C. Goeschel, D. Needham, B. Sexton, D. Thompson, L. Lubomski, J. Marsteller, M. Makary, and E. Hunt, "Creating high reliability in health care organizations," *Health Services Res.*, vol. 41, pp. 1599–1617, Aug. 2006.

[137] T. J. Vogus and D. Iacobucci, "Creating highly reliable health care: How reliability-enhancing work practices affect patient safety in hospitals," *ILR Rev.*, vol. 69, no. 4, pp. 911–938, 2016.

[138] J. Toussaint. (Sep. 2019). *Improving Reliability in Healthcare*. [Online]. Available: https://createvalue.org/articles_and_news/improving-reliability-healthcare/

[139] F. Shi, H. Ning, W. Huangfu, F. Zhang, D. Wei, T. Hong, and M. Daneshmand, "Recent progress on the convergence of the Internet of Things and artificial intelligence," *IEEE Netw.*, vol. 34, no. 5, pp. 8–15, Sep. 2020.

[140] A. P. Singh, N. R. Pradhan, A. K. Luhach, S. Agnihotri, N. Z. Jhanjhi, S. Verma, U. Ghosh, and D. S. Roy, "A novel patient-centric architectural framework for blockchain-enabled healthcare applications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5779–5789, Aug. 2021.

[141] D. Chen, S. Liu, P. Kingsbury, S. Sohn, C. B. Storlie, E. B. Habermann, J. M. Naessens, D. W. Larson, and H. Liu, "Deep learning and alternative learning strategies for retrospective real-world clinical data," *npj Digit. Med.*, vol. 2, no. 1, p. 43, Dec. 2019.

[142] N. G. Maity and S. Das, "Machine learning for improved diagnosis and prognosis in healthcare," in *Proc. IEEE Aerosp. Conf.*, Mar. 2017, pp. 1–9.

[143] I. Tobore, J. Li, L. Yuhang, Y. Al-Handarish, A. Kandwal, Z. Nie, and L. Wang, "Deep learning intervention for health care challenges: Some biomedical domain considerations," *JMIR mHealth uHealth*, vol. 7, no. 8, Aug. 2019, Art. no. e11966.

[144] C. J. Kelly, A. Karthikesalingam, M. Suleyman, G. Corrado, and D. King, "Key challenges for delivering clinical impact with artificial intelligence," *BMC Med.*, vol. 17, no. 1, p. 195, Dec. 2019.

[145] F. Jiang, Y. Jiang, H. Zhi, Y. Dong, H. Li, S. Ma, Y. Wang, Q. Dong, H. Shen, and Y. Wang, "Artificial intelligence in healthcare: Past, present and future," *Stroke Vascular Neurol.*, vol. 2, no. 4, pp. 230–243, 2017.

[146] E. Mezghani, E. Exposito, and K. Drira, "A model-driven methodology for the design of autonomic and cognitive IoT-based systems: Application to healthcare," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 1, no. 3, pp. 224–234, Jun. 2017.

[147] F. Shamout, T. Zhu, and D. A. Clifton, "Machine learning for clinical outcome prediction," *IEEE Rev. Biomed. Eng.*, vol. 14, pp. 116–126, 2021.

[148] Y. Yu, M. Li, L. Liu, Y. Li, and J. Wang, "Clinical big data and deep learning: Applications, challenges, and future outlooks," *Big Data Mining Anal.*, vol. 2, no. 4, pp. 288–305, Dec. 2019.

[149] D. Ravi, C. Wong, F. Deligianni, M. Berthelot, and J. Andreu-Perez, "Deep learning for health informatics," *IEEE J. Biomed. Health Inform.*, vol. 21, no. 1, pp. 4–21, Jan. 2017.

[150] T. L. Rodziewicz, B. Houseman, and J. E. Hipskind, "Medical error reduction and prevention," in *StatPearls [Internet]*. Treasure Island, FL, USA: StatPearls Publishing, Jan. 2021. [Online]. Available: https://www.ncbi.nlm.nih.gov/books/NBK499956/

[151] M. Camara, N. Camara, A. Camara, and F. Traore, "Healthcare settings: The best ways to mitigate errors," *Int. J. Community Med. Public Health*, vol. 1, no. 3, pp. 380–384, 2016.

[152] S. Vala, P. Chemweno, L. Pintelon, and P. Muchiri, "A risk-based maintenance approach for critical care medical devices: A case study application for a large hospital in a developing country," *Int. J. Syst. Assurance Eng. Manage.*, vol. 9, no. 5, pp. 1217–1233, Oct. 2018.

[153] S. Venkataramani *et al.*, "Efficient AI system design with cross-layer approximate computing," *Proc. IEEE*, vol. 108, no. 12, pp. 2232–2250, Dec. 2020.

[154] E. K. Choe and B. Lee, "Toward supporting personalized tracking experiences in healthcare," *Interactions*, vol. 27, no. 1, pp. 84–87, Dec. 2019.

[155] L. F. Rivera, M. Jiménez, P. Angara, N. M. Villegas, G. Tamura, and H. A. Müller, "Towards continuous monitoring in personalized healthcare through digital twins," in *Proc. 29th Annu. Int. Conf. Comput. Sci. Softw. Eng.* Armonk, NY, USA: IBM Corp., 2019, pp. 329–335.

[156] L. Tao and J. Liu, "Understanding self-organized regularities in healthcare services based on autonomy oriented modeling," *Natural Comput.*, vol. 14, no. 1, pp. 7–24, Mar. 2015.

[157] K. Gai, Z. Lu, M. Qiu, and L. Zhu, "Toward smart treatment management for personalized healthcare," *IEEE Netw.*, vol. 33, no. 6, pp. 30–36, Nov. 2019.

[158] N. Kim, J. L. J. Wei, J. Ying, H. Zhang, S. K. Moon, and J. Choi, "A customized smart medical mask for healthcare personnel," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage. (IEEM)*, Dec. 2020, pp. 581–585.

[159] A. Sheth, U. Jaimini, K. Thirunarayan, and T. Banerjee, "Augmented personalized health: How smart data with IoTs and AI is about to change healthcare," in *Proc. IEEE 3rd Int. Forum Res. Technol. Soc. Ind. (RTSI)*, Sep. 2017, pp. 1–6.

[160] W. Hong and W. G. Lee, "Wearable sensors for continuous oral cavity and dietary monitoring toward personalized healthcare and digital medicine," *Analyst*, vol. 145, no. 24, pp. 7796–7808, 2020.

[161] L. Lu, J. Zhang, Y. Xie, F. Gao, S. Xu, X. Wu, and Z. Ye, "Wearable health devices in health care: Narrative systematic review," *JMIR mHealth uHealth*, vol. 8, no. 11, Nov. 2020, Art. no. e18907.

[162] J. U. Knickerbocker, R. Budd, B. Dang, Q. Chen, E. Colgan, L. W. Hung, S. Kumar, K. W. Lee, M. Lu, J. W. Nah, R. Narayanan, K. Sakuma, V. Siu, and B. Wen, "Heterogeneous integration technology demonstrations for future healthcare, IoT, and AI computing solutions," in *Proc. IEEE 68th Electron. Compon. Technol. Conf. (ECTC)*, May 2018, pp. 1519–1528.

[163] K. Paranjape, M. Schinkel, and P. Nanayakkara, "Short keynote paper: Mainstreaming personalized healthcare–transforming healthcare through new era of artificial intelligence," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 7, pp. 1860–1863, Jul. 2020.

[164] J. P. Rowe and J. C. Lester, "Artificial intelligence for personalized preventive adolescent healthcare," *J. Adolescent Health*, vol. 67, no. 2, pp. S52–S58, Aug. 2020.

[165] E. Gómez-González, E. Gomez, J. Márquez-Rivas, M. Guerrero-Claro, I. Fernández-Lizaranzu, M. I. Relimpio-López, M. E. Dorado, M. J. Mayorga-Buiza, G. Izquierdo-Ayuso, and L. Capitán-Morales, "Artificial intelligence in medicine and healthcare: A review and classification of current and near-future applications and their ethical and social impact," 2020, *arXiv:2001.09778*.

[166] Z. Ahmed, K. Mohamed, S. Zeeshan, and X. Dong, "Artificial intelligence with multi-functional machine learning platform development for better healthcare and precision medicine," *Database*, vol. 2020, no. 2020, Mar. 2020.

[167] I. in Healthcare Market. (Jun. 2020). *Markets and Markets*. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/iot-healthcare-market-160082804.html

[168] (Dec. 2020). *Wi-Fi 6 and 5G*. [Online]. Available: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/802-11ax-solution/pdf/c05-742082-things-to-know-about-wifi6.pdf

[169] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of security and privacy issues of Internet of Things," 2015, *arXiv:1501.02211*.

[170] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) security: Current status, challenges and prospective measures," in *Proc. 10th Int. Conf. for Internet Technol. Secured Trans. (ICITST)*, Dec. 2015, pp. 336–341.

[171] M. Farooq, M. Waseem, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A review on Internet of Things (IoT)," *Int. J. Comput. Appl.*, vol. 113, no. 1, pp. 1–7, 2015.

[172] G. Hattab and D. Cabric, "Energy-efficient massive IoT shared spectrum access over UAV-enabled cellular networks," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5633–5648, Sep. 2020.

[173] M. Furdek, L. Wosinska, and R. Goścień, K. Manousakis, M. Aibin, K. Walkowiak, S. Ristov, M. Gushev, and J. L. Marzo, "An overview of security challenges in communication networks," in *Proc. 8th Int. Workshop Resilient Netw. Design Modeling (RNDM)*, Sep. 2016, pp. 43–50.

[174] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks," in *Proc. 3rd Int. Conf. Electron. Design (ICED)*, Aug. 2016, pp. 321–326.

[175] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of Internet of Things (IoT)," *Int. J. Comput. Appl.*, vol. 111, no. 7, pp. 1–6, Feb. 2015.

[176] M. Surya Virat, S. M. Bindu, B. Aishwarya, B. N. Dhanush, and M. R. Kounte, "Security and privacy challenges in Internet of Things," in *Proc. 2nd Int. Conf. Trends Electron. Informat. (ICOEI)*, May 2018, pp. 454–460.

[177] S. Rostampour, N. Bagheri, M. Hosseinzadeh, and A. Khademzadeh, "A scalable and lightweight grouping proof protocol for Internet of Things applications," *J. Supercomput.*, vol. 74, no. 1, pp. 71–86, Jan. 2018.

[178] A. I. Newaz, A. K. Sikder, L. Babun, and A. S. Uluagac, "HEKA: A novel intrusion detection system for attacks to personal medical devices," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2020, pp. 1–9.

[179] W. N. Price and I. G. Cohen, "Privacy in the age of medical big data," *Nature Med.*, vol. 25, no. 1, pp. 37–43, 2019.

[180] N. Martinez-Martin, T. R. Insel, P. Dagum, H. T. Greely, and M. K. Cho, "Data mining for health: Staking out the ethical territory of digital phenotyping," *npj Digit. Med.*, vol. 1, no. 1, pp. 1–5, Dec. 2018.

[181] C. Lamanna and L. Byrne, "Should artificial intelligence augment medical decision making? The case for an autonomy algorithm," *AMA J. Ethics*, vol. 20, no. 9, pp. 902–910, 2018.

[182] R. Dasoriya, J. Rajpopat, R. Jamar, and M. Maurya, "The uncertain future of artificial intelligence," in *Proc. 8th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence)*, Jan. 2018, pp. 458–461.

[183] N. Kumar, N. Kharkwal, R. Kohli, and S. Choudhary, "Ethical aspects and future of artificial intelligence," in *Proc. Int. Conf. Innov. Challenges Cyber Secur. (ICICCS-INBUSH)*, Feb. 2016, pp. 111–114.

[184] K. Hasan, S. Shetty, and S. Ullah, "Artificial intelligence empowered cyber threat detection and protection for power utilities," in *Proc. IEEE 5th Int. Conf. Collaboration Internet Comput. (CIC)*, Dec. 2019, pp. 354–359.

[185] S. Yeasmin, "Benefits of artificial intelligence in medicine," in *Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, May 2019, pp. 1–6.

[186] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?" *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 41–49, Sep. 2018.

[187] P. Esmaeilzadeh, "Use of AI-based tools for healthcare purposes: A survey study from consumers' perspectives," *BMC Med. Inform. Decis. Making*, vol. 20, no. 1, pp. 1–19, 2020.

NAJMA TAIMOOR received the Master's degree in healthcare and IT from the University of Applied Sciences, Austria with Distinction. She is currently pursuing the Ph.D. degree with the Technische Universität Vienna (TU Wien), Austria. Her Master's thesis was co-developed with the University of Surrey, U.K., in the frame of the Erasmus grant. Her research interests include AI and IoT-based reliable healthcare systems.

SEMEEN REHMAN received the Ph.D. degree from the Karlsruhe Institute of Technology (KIT), Germany, in 2015, and the Habilitation degree in embedded systems from the Technische Universität Wien (TU Wien), in 2020. Since 2015, she has been a Postdoctoral Researcher with the Technische Universität Dresden (TU Dresden) and KIT, Germany. She is currently with the Faculty of Electrical Engineering, TU Wien, as a Tenure-Track Assistant Professor. She has coauthored one book, multiple book chapters, and more than 50 publications in premier journals and conferences. Her main research interests include dependable systems, cross-layer design for error resiliency with a focus on run-time adaptations, emerging computing paradigms, such as approximate computing, hardware security, energy-efficient computing, embedded systems, MPSoCs, the Internet of Things, and cyber-physical systems. She has received the CODES+ISSS 2011 and 2015 Best Paper Awards, the DATE 2017 Best Paper Award Nomination, several HiPEAC Paper Awards, the Richard Newton Young Student Fellow Award from DAC 2015, and the Research Student Award from KIT, in 2012. She has served as the TPC Track Chair for the ISVLSI 2020 and 2021 conference. She also served as the TPC member for multiple premier conferences on design automation and embedded systems, such as DAC, DATE, CASES, ASPDAC, and VLSID. She has chaired/co-chaired multiple sessions at the DATE conference, from 2017 to 2019.

• • •