

MBZUAI

Digital.Commons@MBZUAI

---

Machine Learning Faculty Publications

Scholarly Works

---

4-12-2022

## Internet of Things Device Capabilities, Architectures, Protocols, and Smart Applications in Healthcare Domain: A Review

Md. Milon Islam

*University of Waterloo, Canada*

Sheikh Nooruddin

*University of Waterloo, Canada*

Fakhreddine (Fakhri) Karray

*Mohamed bin Zayed University of Artificial Intelligence*

Ghulam Muhammad

*King Saud University, Saudi Arabia*

Follow this and additional works at: <https://dclibrary.mbzuaai.ac.ae/mlfp>



Part of the [Artificial Intelligence and Robotics Commons](#)

Preprint: arXiv

Archived with thanks to arXiv

Preprint License: CC by 4.0

Uploaded 24 March 2022

---

### Recommended Citation

M.M. Islam, S. Nooruddin, F. Karray, and G. Muhammad, "Internet of Things Device Capabilities, Architectures, Protocols, and Smart Applications in Healthcare Domain: A Review", arXiv, Apr 2022, doi: arXiv:2204.05921v1

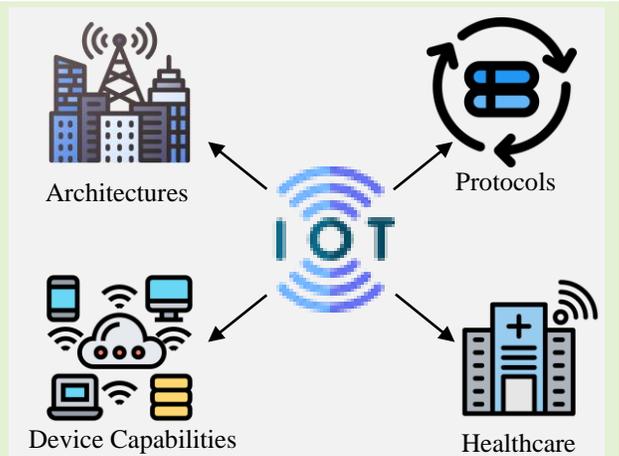
This Article is brought to you for free and open access by the Scholarly Works at Digital.Commons@MBZUAI. It has been accepted for inclusion in Machine Learning Faculty Publications by an authorized administrator of Digital.Commons@MBZUAI. For more information, please contact [libraryservices@mbzuaai.ac.ae](mailto:libraryservices@mbzuaai.ac.ae).

# Internet of Things Device Capabilities, Architectures, Protocols, and Smart Applications in Healthcare Domain: A Review

Md. Milon Islam, Sheikh Nooruddin, Fakhri Karray, *Fellow, IEEE*, and Ghulam Muhammad, *Senior Member, IEEE*

**Abstract**—Nowadays, the Internet has spread to practically every country around the world and is having unprecedented effects on people’s lives. The Internet of Things (IoT) is getting more popular and has a high level of interest in both practitioners and academicians in the age of wireless communication due to its diverse applications. The IoT is a technology that enables everyday things to become savvier, everyday computation towards becoming intellectual, and everyday communication to become a little more insightful. In this paper, the most common and popular IoT device capabilities, architectures, and protocols are demonstrated in brief to provide a clear overview of the IoT technology to the researchers in this area. The common IoT device capabilities including hardware (Raspberry Pi, Arduino, and ESP8266) and software (operating systems, and built-in tools) platforms are described in detail. The widely used architectures that have been recently evolved and used are the three-layer architecture, SOA-based architecture, and middleware-based architecture. The popular protocols for IoT are demonstrated which include CoAP, MQTT, XMPP, AMQP, DDS, LoWPAN, BLE, and Zigbee that are frequently utilized to develop smart IoT applications. Additionally, this research provides an in-depth overview of the potential healthcare applications based on IoT technologies in the context of addressing various healthcare concerns. Finally, this paper summarizes state-of-the-art knowledge, highlights open issues and shortcomings, and provides recommendations for further studies which would be quite beneficial to anyone with a desire to work in this field and make breakthroughs to get expertise in this area.

**Index Terms**— Internet of Things, Device Capabilities, IoT Architecture, Communication Protocol, Healthcare Applications.



## I. Introduction

THE IoT concept represents a set of Internet-connected devices that are empowered with computing capability, are easily recognizable, and can share data over the Internet without the need for physical contact. The IoT revolution has resulted in unprecedented levels of interconnection among devices, allowing for the development of smart environments. The smart connectivity with the existing network, as well as

context-aware information processing employing network resources, are essential components of IoT [1], [2]. The IoT allows physical things to see, hear, think, and execute a variety of tasks by allowing them to “speak” to one another, exchange information data, and make choices. The concept of IoT turns these devices from being conventional to smart by leveraging its wide range of technologies including embedded applications, Internet protocol and applications, wireless communications, distributed networks, and sensor technologies [3], [4]. An important advancement of the current Internet into a network of interconnected objects is that it not only comes into contact with the physical surroundings via actuation, controlling, and monitoring, nor merely extracts information from the surroundings, but it also uses traditional network requirements to enhance data transfer, predictive analysis, and communication [4], [5]. The IoT covers a huge number of applications including healthcare, automotive, utilities, smart cities, wearables, smart homes, and smart farming [6], [7]. Numerous research projects, enterprises, and businesses are currently engaged in the creation of various IoT features to accommodate the growing evolving needs that

Md. Milon Islam, and Sheikh Nooruddin are with the Centre for Pattern Analysis and Machine Intelligence, Department of Electrical and Computer Engineering, University of Waterloo, ON, N2L 3G1, Canada (e-mail: milonislam@uwaterloo.ca, and sheikh.nooruddin@uwaterloo.ca).

Fakhri Karray is with the Centre for Pattern Analysis and Machine Intelligence, Department of Electrical and Computer Engineering, University of Waterloo, ON, N2L 3G1, Canada and Mohamed bin Zayed University of Artificial Intelligence, Abu Dhabi, United Arab Emirates (e-mail: karray@uwaterloo.ca).

Ghulam Muhammad is with the Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia and Center of Smart Robotics Research, King Saud University, Riyadh, Saudi Arabia (e-mail: ghulam@ksu.edu.sa).

emerge with such rapid development.

A healthcare platform is described as a combination of hardware and software components that work together to give a wide range of healthcare services and applications to people including healthcare professionals and patients, to promote health in an efficient and widespread manner [8], [9]. Nowadays, there are numerous healthcare frameworks available that integrate various technologies to monitor multiple human bio-physical symptoms and environmental data utilizing various wireless communications techniques including ZigBee, 5G, Bluetooth, and Wi-Fi [10], [11]. IoT technology supports healthcare systems by allowing people to remain at smart homes and be monitored in real-time rather than being admitted to hospitals or clinics that reduces the emergency costs [12], [13]. There are several advantages of IoT technologies to design smart healthcare systems such as ease of access, ensuring patient comfort and safety, and reducing patient's burden in hospitals. In general, IoT enables networks of smart devices, cloud applications, and solutions to make data transfer and storage easier. The most promising applications of IoT in the area of healthcare include remote monitoring, smart medical device, smart homes, as well as wearable devices. In recent years, several academic and industry researches on IoT interoperability including the healthcare domain have been done, with an emphasis on the standardization of communication protocols to offer interoperability of diverse devices, networks, and data structures [14], [15]. To ensure QoS in healthcare systems, IoT should incorporate some aspects such as standardization of reliable communication protocols, enhanced mobile and wearable devices, and low-cost as well as low-power embedded processors [16], [17]. The IoT communication architecture could be the primary enabling mechanism for decentralized pervasive healthcare applications, considering the prevailing availability of distant wireless healthcare platforms and the rising topic of electronic patientcare datasets [18], [19].

This paper is aimed at highlighting the fundamental issues of IoT device capabilities, architectures, protocols, and healthcare applications in detail. The IoT device incorporates all the necessary components for hardware and software platforms. The hardware platform describes the most popular portable processing devices such as Raspberry Pi, Arduino, and ESP8266 highlighting some significant features including power requirement, memory capacity, and processing power. The software platform is described focusing the operating systems for small embedded devices and built-in software for IoT-related tasks. The operating systems named Contiki, Mbed, RIOT, Embedded Linux, and Windows 10 IoT are described here with their distinguished features. The popular and widely used built-in tools for IoT smart applications include DeviceHive, Kaa, ThingsBoard, AWS IoT, and Google Cloud IoT. The IoT architectures such as three-layer, SoA-based, and middleware-based architectures are depicted to provide cutting-edge insights. The three-layer architecture contains the layers of perception, network, and application. Additionally, the SoA-based architecture comprises of a

service layer along with the layers of the three-layer architecture. The middleware and business layers are the additional layer in the middleware-based architecture over the three-layer architecture. The IoT communication protocols are also demonstrated here to provide an overview of communication interfaces. The popular eight protocols that are described in this paper are CoAP, MQTT, XMPP, AMQP, DDS, LoWPAN, BLE, and Zigbee. The most promising healthcare applications for monitoring, diagnosis, and treatment for individuals using IoT technologies are demonstrated. The major applications include bio-physical parameter monitoring, chronic disease detection, medication management, telehealth, as well as home and elderly care. The current challenges for IoT technologies and potential future trends are explored to find out the research gaps and potential solutions to develop smart applications. The key contributions of the paper are highlighted as follows.

- (i) Providing a comprehensive discussion on IoT device capabilities highlighting the area of hardware and software systems including the processing capabilities, operating systems, and built-in tools.
- (ii) Addressing core technologies for IoT architectures that are the fundamental issues in diverse application domains of IoT and a detailed discussion on it.
- (iii) Analyzing typical IoT communication protocols that deal with data transmission concerns via networks, as well as providing an overview of each.
- (iv) Exploring the in-depth analysis of the most recent and promising IoT-based healthcare applications incorporating different architectures and protocols for monitoring, diagnosis, and treatment of the patients in hospitals as well as smart home environments.
- (v) Presenting a study of the major open issues for application approaches in the IoT context, as well as the future trends to provide the scope of further research for smart applications.

The remaining parts of the paper read as follows. The paper collection and selection criteria are demonstrated in section II. Section III provides the concept of IoT device capabilities with proper illustration of hardware and software platforms. The architectures that are available in recent times to develop smart systems are described in section IV. Section V demonstrates the IoT protocols that are generally used to transfer data over the Internet. The healthcare applications of IoT technology are briefly described in section VI. Section VII demonstrated the open discussions of the IoT technology with the current challenges as well as the potential future works. Section VIII concludes the paper.

## II. PAPER COLLECTION AND SELECTION

This research was limited to peer-reviewed research works published in reputed international venues mostly within the years from 2017 to 2022 and written in English. Some notable sources used for this research are Google Scholar, EMBASE, PubMed, and NCBI. The most used search keywords were "IoT Overview", "IoT Security Issues", "IoT architectures", "IoT in Healthcare", "IoT Operating Systems", "Challenges in IoT", "Industrial IoT", and "Smart Applications using IoT".

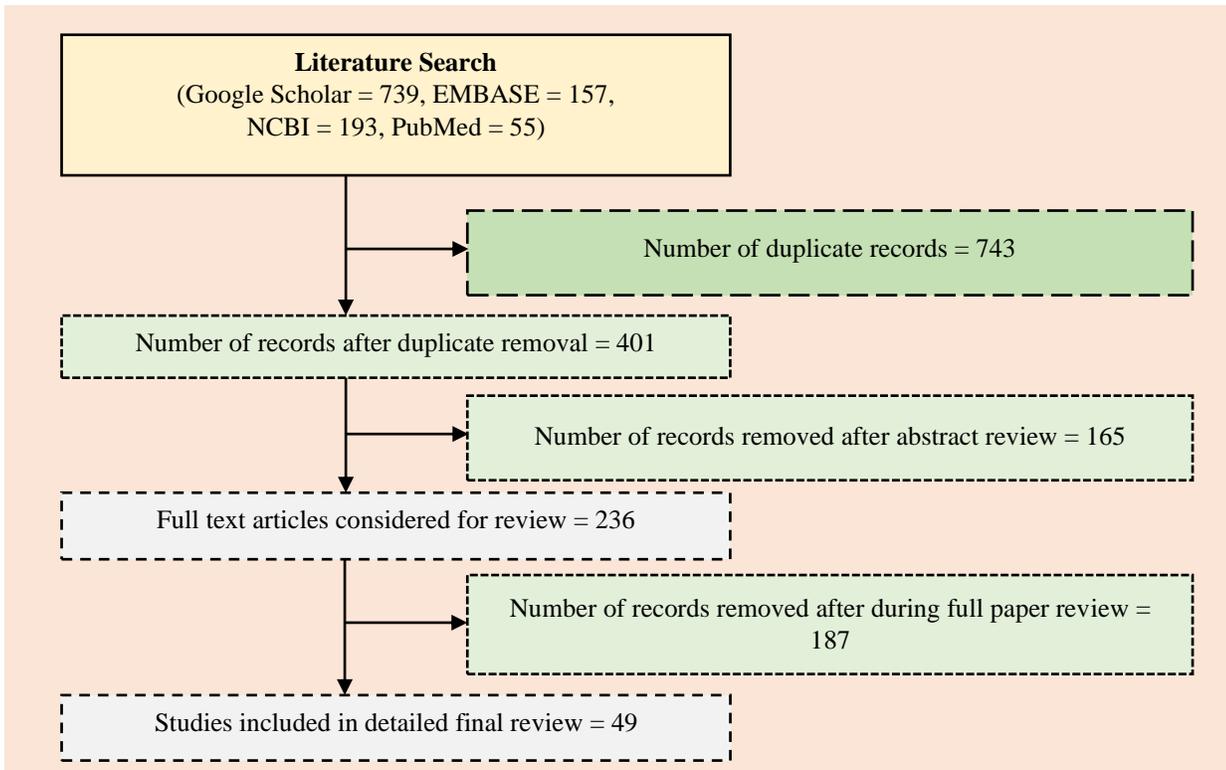


Fig. 1. Flow diagram showing article selection for final review. The final selection is done based on the duplicate records, abstract review, and full paper review.

We also manually searched various web search engines such as Google, DuckDuckGo, and Bing and books, articles, online magazines, online reports from reputable sources to provide various statistics. The abstracts, titles, keywords, and overall structures of the papers were analyzed to eliminate duplicates. We also eliminated publications that were beyond the scope of this work. Fig. 1 shows the article selection process of the detailed review paper from the initial search stage. Only a very small number of papers were selected for review from the initial high number of search results. The rejected papers were removed based on duplication, and out of focus of this work.

### III. IOT DEVICE CAPABILITIES

In general, an IoT framework comprises of devices that perform sensing, actuation, control, and surveillance tasks. IoT devices are able to transmit data to other devices and applications over the Internet, or they can retrieve data from other connected devices and process it locally or on a cloud server after sending it to centralized servers. The tasks are completed on the local server or within the IoT architecture depending on some temporal and spatial restrictions such as memory, communication delays, deadlines, computational power, and speed of operation. An IoT device may have multiple interfaces for communicating with other devices, in both wired and wireless mode. The common interfaces that are equipped with most of the IoT devices are I/O interfaces for sensors, Internet connectivity interfaces, memory and storage interfaces, and audio/video interfaces. There are various types of IoT objects such as wearable sensors, accelerometers, cameras, smart watches, smart locks, Global Positioning

System (GPS), and LED lights that are available for smart applications. Mostly all IoT devices produce large amounts of data in various forms, which while analyzed by data analytics engines, carries important information that can be used to guide local or remote activities. The IoT device capabilities highlighting hardware and software platform is shown in Fig. 2. In the following section, the device capabilities including hardware and software platforms are demonstrated in brief.

#### A. Hardware

The hardware components for the Internet of Things have arrived in a variety of shapes and sizes, depending on the tasks at hand. For instance, the core CPUs are used to operate the phones, the sensors are utilized to perceive data from the physical environment, and the data are processed and analyzed on the edge devices. In the case of wired mode, the hardware aspects are the essential components of the IoT platform, and the capabilities of these devices have only grown in significance as IoT has progressed. The main hardware kits that are widely used to develop IoT applications are described here focusing on some properties such as processing power, memory capacity, and power requirement.

##### (i) Raspberry Pi

Raspberry Pi is a series of single-board computers that compress a lot of processing power into a tiny box and offer desktop-like functionality [20]. The components of Raspberry Pi vary based on its version. In Raspberry Pi B+ model, there are four USB ports, two ports for the camera, an Ethernet port, an audio jack port, and a HDMI port. To implement real case studies, there are 17 General Purpose Input Output (GPIO)

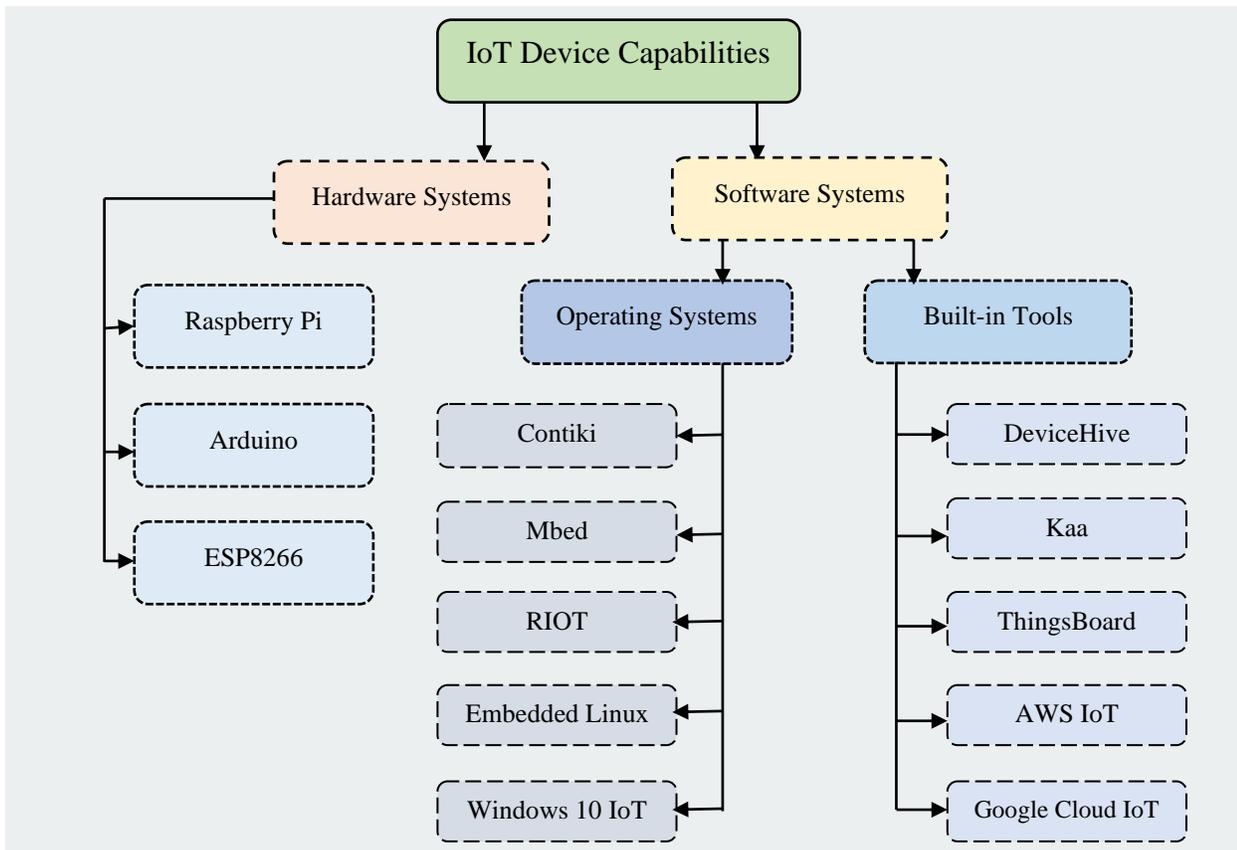


Fig. 2. IoT device capabilities considering hardware and software platforms. The hardware platform includes several types of tiny processing devices such as Raspberry Pi, Arduino, and ESP8266. The software module comprises several operating systems and built-in tools.

pins that are available to connect with any electronic components such as LEDs, sensors, switches, and motors. The minimum required logic level for the Raspberry Pi is almost 3.3V. In general, it is run over the Raspbian operating system. Additionally, it is also compatible with other operating systems such as Lakka, RaspBSD, and RetroPie [21]. The programming languages that are supported in Raspberry Pi are Python, Java, C++, and C. The combination of GPIO pins with the Linux operating system gives this device a lot of flexibility and gives users a lot of choices. The CPU speed of the standard Raspberry Pi model is 700 MHz to 1.4 GHz, memory capacity is 256 MB to 4 GB, and the power requirement is 2.5 Amp. These measures are varied based on the version of the Raspberry Pi model. The Raspberry Pi is well-suited for a wide range of applications due to its high connectivity, ease of use, portability, low power consumption, high flexibility, and high transferability [22]. However, there is no power button to keep it in sleep mode while it becomes idle, no built-in ADC, and replicability is quite hard for this device.

### (ii) Arduino

Arduino is a popular and frequently used open-source electronics framework based on simple hardware and software that can be utilized to develop electronic projects. It offers a wide variety of products, from straightforward 8-bit microcontroller boards to wearable technologies, IoT components, and 3-D printing [23]. The set of instructions to complete any tasks are executed through microcontrollers.

There are several versions of Arduino such as UNO, micro, pro, mega, and nano available in the market for electronic system development where the use of the Arduino model varies based on the nature of the applications. It is easily compatible with MAC, windows as well as Linux platforms. A type B USB cable is utilized to do programming in the Arduino board with the support of an IDE [24]. The supported language for Arduino is C++ where the fundamental issue of peripherals such as sensors and actuators are controlled through the use of header files. Arduino Uno has analog pins, digital pins, a USB connection, a reset button, a crystal oscillator, and a power jack. Arduino is highly suited to perceive data from physical environments i.e., analog data [25].

### (iii) ESP8266

ESP8266 is a mini-sized, Wi-Fi enabled device with full TCP/IP stack and microcontroller capability which is frequently used for embedded development in IoT environments [26]. This device can host an application that offloads all Wi-Fi network services to another underlying hardware. The Wi-Fi module of ESP8266 is pre-programmed with an ESP-AT command set firmware that enables any Arduino device to get a Wi-Fi connection. It runs at 80 MHz and uses a 32-bit RISC CPU (reduced instruction set computer) based on the Tensilica Xtensa L106. The boot ROM, instruction RAM, and data RAM size of ESP8266 are 64 KB, 64 KB, and 96 KB respectively.

TABLE I  
IoT HARDWARE COMPONENTS WITH SOME PROPERTIES

Property	Raspberry Pi	Arduino	ESP8266
Programming	Python/Java/C++	C++	C++/Lua
Wi-Fi	USB dongle	Shield or ESP8266	Built-in
Code Distribution	In-Situ	USB/SPI/Serial	Serial/OTA
Storage	SD-card	Built-in	Built-in
I/O	17 GPIO	Arduino UNO: 13 GPIO/6 ADC	10 GPIO/1 ADC
CPU speed	700 MHz to 1.4 GHz	16 MHz	80 MHz
CPU	ARM Cortex-A7, ARM Cortex A-53, ARM Cortex-A72	Atmel AVR, ARM Cortex-M0+, ARM Cortex-M3, Intel Quark	Tensilica L106 32-bit RISC processor
Memory Capacity (RAM)	256 MB-4 GB	16 KB-64 MB	128 KB-4 MB
Power Requirement	5V, 2.5 Amp	5V, 250 mA	3.3V, 70.5 mA
Cost	Expensive (\$35)	Moderate (\$3-\$30)	Low cost (\$3)

The Serial Peripheral Interface (SPI) accesses the external flash memory. ESP8266 is quite fit for the low-cost systems [27] that do not require a high amount of CPU support, huge storage, some special features such as camera, USB, and HDMI ports.

Table I shows the different properties including CPU speed, memory capacity, power requirement, supported programming languages, and storage of the above-mentioned hardware components.

## B. Software

In general, IoT software outlines the key aspects of communication networks and action via numerous channels, integrated devices, partner systems, and development tools. IoT software is the underlying platform that allows a connected device to capture and communicate data in real-time where the data are generally processed by computers and relevant applications. The connected devices can operate effectively owing to the intelligence that IoT software ensures. Smart devices are limited to their computing power and in such scenarios, intelligence is ensured through cloud computing technology where the IoT software is located. The operating systems along with built-in tools which are the parts of IoT software are described here.

### (i) Operating Systems

An IoT Operating System (OS) is a part of software platforms that ensures how IoT smart devices interact with users and handle all software and hardware resources. IoT OSs are integrated operating systems that are intended to work in small IoT devices with limited memory and low processing capacity. IoT devices can interact with cloud platforms and other intelligent devices over a global network thanks to embedded operating systems. The operating systems for a particular application are chosen based on some performance measures including flexibility, compatibility, reliability, simplicity, and consistency. The popular IoT operating systems are demonstrated here to provide a short overview of embedded operating systems.

#### 1) Contiki

Contiki is a freely available operating system that is well-known for its way of interacting with extremely small, low-power, and cost-effective embedded systems to the Internet [28]. The programming language that is used in Contiki is C.

It supports multithreading via protothread, and the processes are managed through cooperative or preemptive scheduling. Generally, multiple stacks are supported in Contiki including some features such as 6LoWPAN, CoAP, and IPv6 [29]. This operating system is appropriate for developing complex wireless systems due to its high memory efficiency.

#### 2) Mbed

Mbed operating system is a publicly available, open-source OS that is quite popular for its integration with ARM processors and has a wide range of connectivity features such as Wi-Fi, Ethernet, 6LoWPAN, Cellular, and Bluetooth [30]. It is particularly tailored for 32-bit ARM processors. This operating system has a multilayer security system that provides users with a high level of reliability. Mbed OS is well-suited to IoT applications on ARM cortex M-based devices, as it preserves code clean and portable features [31]. It is a popular IoT OS due to its low system requirements and compatibility with a variety of development kits.

#### 3) RIOT

RIOT is another widely used and popular operating system specifically designed for embedded devices [32]. This OS targets wireless sensor networks as it is developed based on a microkernel architecture named FireKernel. It ensures the usage of multithreading and SSL/TSL libraries, as well as provides the facilities of the use of 8, 16, and 32-bit processors. The supported language for RIOT is C and C++. RIOT can run as a Linux or macOS process as there is a dedicated port for this OS. RIOT enables modular design and provides access to separate hardware abstraction for minimal memory and energy consumption [33].

#### 4) Embedded Linux

Embedded Linux is a significantly modified version of the Linux kernel, designed specifically for embedded devices. The compact size and low power consumption of this OS make it well-suited for fulfilling all the requirements of IoT devices such as tablets, navigational devices, and wireless routers [34]. It requires a small amount of storage like 100 KB of memory that makes it quick and dynamic. In the IoT OS world, this OS also offers an unparalleled level of customization. Embedded Linux OS is easily compatible with any single-board computer such as Raspberry Pi (Raspbian, Ubuntu Core, OSMC, and Gentoo). Linux distros are popular options for IoT applications

**TABLE II**  
A SHORT LOOK AT THE IOT OPERATING SYSTEMS

Operating Systems	Features	Provider	License	Processor	Use Cases
Contiki	Open-source, free	ThingSquare	3-clause BSD	ARM Cortex-M, MSP430, AVR, and x86.	Networked memory-constrained systems
Mbed	ARM-based, high-grade security	ARM	Apache 2.0	ARM Cortex-M	For portable code
RIOT	Open-source, full multithreading	FU Berlin	LGPLv2.1	ARM Cortex-M, MSP430, ARM7, AVR, x86, and Cortex-M23.	Can be run as a MacOS process
Embedded Linux	Linux kernel, free	Multiple providers	GPL, and GPLv2	ARM Cortex-A8, ARM Cortex A-53, and Intel Core i3, i5, i7.	Versatile-can be used for various use cases
Windows 10 IoT	Proprietary, high-grade security	Microsoft Corporation	Commercial	ARM Cortex-A7, Snapdragon 400, ARM Cortex-A53	Ideal for heavy-duty industrial use cases

due to some performance factors such as flexibility, consistency, architectural layers, cloud support, and visualization [35].

### 5) Windows 10 IoT

Windows 10 IoT is a product of Microsoft Windows 10 operating system, but it is dedicatedly designed for IoT devices [36]. Windows IoT is divided into two parts: Windows 10 IoT core, which is considered to interact with tiny embedded devices, and Windows 10 IoT Enterprise, which is developed for industrial use. Windows 10 IoT includes a user-friendly interface, more user control than some other OSs, and is universally recognized as a capable IoT operating system among IoT experts. Windows OS is a quite better choice over free or open-source ones whenever reliability and security become critical issues [37].

Table II provides an overview of the discussed IoT operating systems including some dominant features such as accessibility, provider, license, processor, and use cases.

#### (ii) Built-in-Tools

Generally, IoT software has two main attributes such as (i) Connectivity with wired or wireless devices via Bluetooth, ZigBee, Ethernet, 5G/6G, or satellite communications. (ii) Automated communication between the hardware, devices, or machinery without human involvement to initiate an operation or carry out actions. The available built-in tools are developed based on these two characteristics to carry out automated data analysis and transfer, as well as autonomous response. The most popular IoT built-in tools are described here to provide in-depth knowledge to the researchers.

##### 1) DeviceHive

DeviceHive is a publicly accessible platform that offers communication and management tools for connected devices. There are several things included in DeviceHive such as communication layer, control software, multi-platform modules and users to launch smart home development, remote control and monitoring tool, and telemetry [38]. DeviceHive is compatible with Python, Node.js, and Java client modules. It uses the REST, WebSocket, and MQTT protocols to connect with other devices. This platform is a modular, hardware, and cloud independent micro service-oriented solution with access control APIs in several protocols that enable users to monitor, control, and analyze the behavior of their devices.

##### 2) Kaa

Kaa is developed for enabling smart devices to communicate with each other across a big cloud. Kaa is an open-source development tool, and it is hardware-oriented i.e., it is well-suited for any hardware components such as sensors, gateways, and devices. Kaa's multi-purpose middleware enables users to develop IoT solutions, application support, and a variety of intelligent devices [39]. The set-up of Kaa tool is quite easy and it provides a large number of features that can be integrated into the platform easily. Kaa is a scalable IoT platform that uses a microservice design to provide obvious layers of abstraction, flexibility, and scalability [40].

##### 3) ThingsBoard

ThingsBoard is a free server-side built-in tool for data collection, processing, monitoring, and device management [41]. It is deployable in any smart application including personal and commercial purposes. ThingsBoard supports several protocols such as CoAP, MQTT, and HTTP. The IoT devices are easily connected to the platform via ThingsBoard gateway. Although the back-end of ThingsBoard is written in Java, it supports several micro services based on Node.js. Some of the major reliant features of ThingsBoard are scalable, fault-tolerant, robust and efficient, adaptable, and resilient [42]. In practical scenarios, it is well-suited for predictive analytics tasks such as smart farming, smart metering, and smart energy.

##### 4) AWS IoT

The Amazon Web Services (AWS) IoT tool is a reliable and secure development platform for industrial, business, and retail solutions. This platform can be used to analyze and manage data from Internet-connected devices and sensors in residences, businesses, healthcare, automobiles, and other locations [43]. It supports HTTP, LoRaWAN, the lightweight communication protocol, and MQTT to publish and subscribe to messages. This tool incorporates layers of security like encryption, secure access, constant monitoring, and audits. AWS IoT is able to handle smart objects and trillions of signals, and it can securely and efficiently interpret and transmit those signals to AWS endpoints and other devices [44].

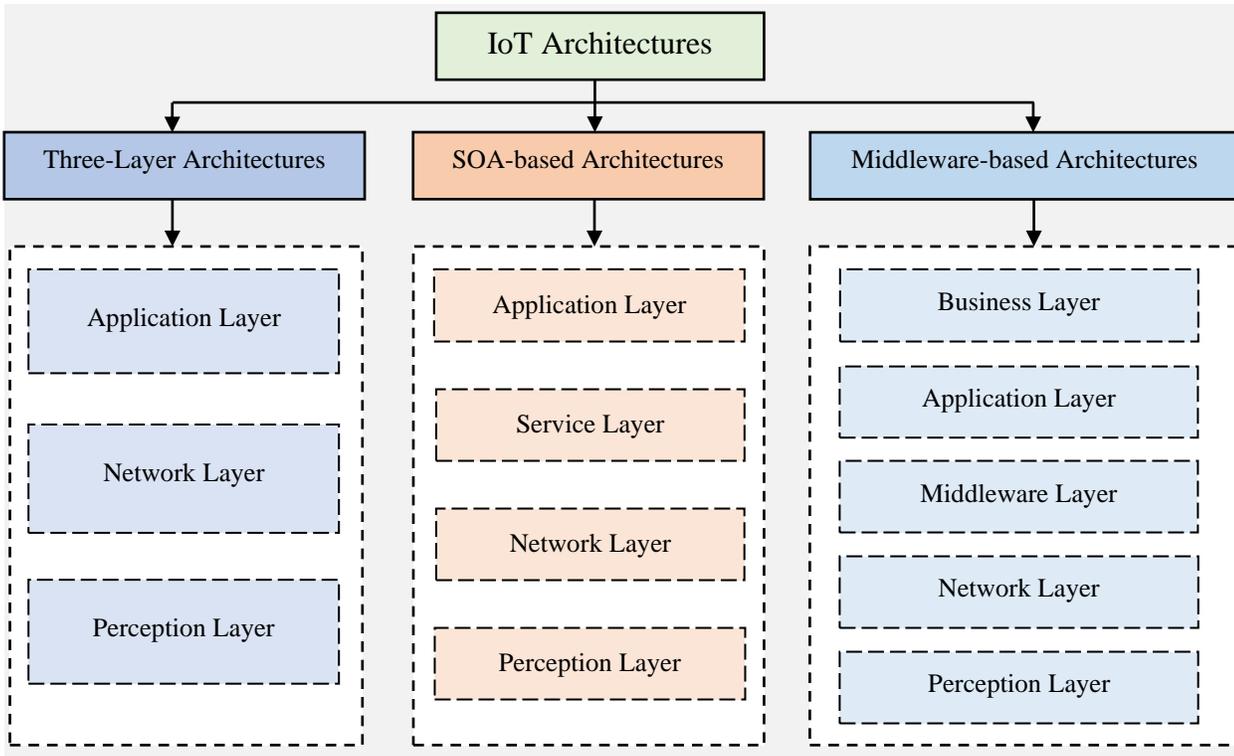


Fig. 3. Most common and frequently used IoT architectures that incorporate the three-layer architecture, SOA-based architecture, and middleware-based architecture.

### 5) Google Cloud IoT

Google Cloud provides scalable services that are quite managed and incorporated with IoT devices. The functionalities of this tool include connecting, preserving, and investigating data at the edge and in the cloud. The common aspects of Google Cloud IoT are data warehousing and quick querying, streaming and batch analysis, device connectivity and management, as well as Artificial Intelligence (AI) and Machine Learning (ML) models [45]. This platform is capable of predicting equipment maintenance and optimizing operations, as well as monitoring resources in real-time. Google Cloud IoT covers a wide range of applications including predictive analytics, logistics and supply chain management, smart cities and infrastructures, as well as real-time asset surveillance [46].

## IV. IOT ARCHITECTURES

The Internet of Things should be competent at networking billions or trillions of diverse things over the Internet, therefore, a flexible architectural pattern is crucial. Some of the major factors like reliability, scalability, privacy and security, quality of service (QoS), and data storage should be considered at the time of developing the architecture of an IoT network [47], [48]. To fulfill the demand of the defined key features, several research groups have proposed several IoT architectures. The ever-growing number of potential architectures has been unable to settle on a standard model [49]. There is no specific base architectural pattern till now despite numerous standardization initiatives. This is because of its wide area of applications having

different design patterns and variables/factors to measure the performance of the existing systems. Fig. 3 depicts the most common and widely used IoT architectures, which are explained as follows.

### A. Three-Layer Architectures

The most fundamental architecture is the three-layer architecture which was developed in the beginning periods of research in the IoT area [50], [51]. This architecture is divided into three base architectures such as perception layer, network layer, and application layer which are demonstrated below.

#### 1) Perception Layer

In the IoT ecosystem, the perception layer is sometimes referred to as the sensor layer, and it is deployed in the bottom layer. The perception layer interferes with the environments via smart devices like sensors, actuators, cameras, and GPS terminals to collect and process data. This layer's primary functions include connecting devices to the IoT framework, measuring, and processing real-time physical parameters (data) from connected things via intelligent devices, and transmitting data to the higher layer via its interfaces [52], [53]. In the perception layer, heterogeneous devices are configured using standardized plug-and-play techniques [54]. The major success of IoT, known as big data, begins in this layer.

#### 2) Network Layer

The network layer, also known as the transmission layer and incorporated in the middle layer of the IoT framework, is referred to as the core of the IoT ecosystem [55]. The network

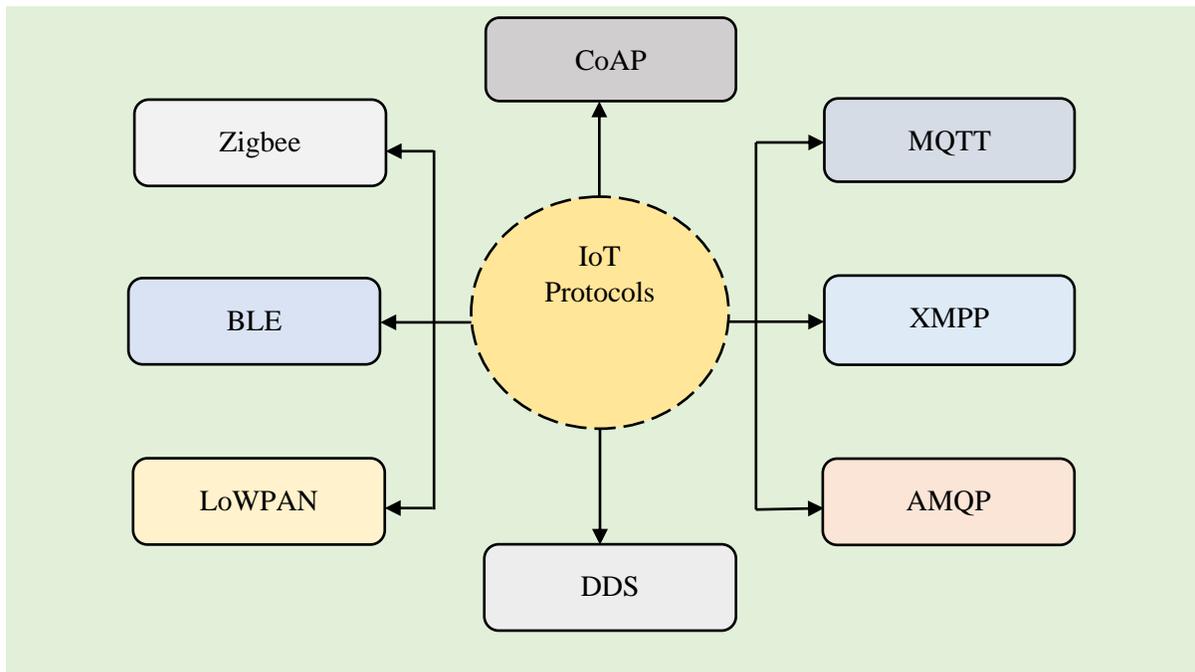


Fig. 4. Most common emerging IoT communication protocols that are extensively used to develop smart IoT applications.

layer serves as a link between the perception layer and the application layer, allowing data to be transferred to IoT servers, applications, and devices through interconnected networks. The network layer consists of different communication standards like Wi-Fi, Bluetooth, and ZigBee [56] and IoT objects like gateway, hub, and switching [57]. The use of wireless protocols is very important in this layer because wireless devices can be deployed in critical environments with less material and human effort [58]. This layer generally transmits/receives data to/from various applications via interfaces/gateways using a variety of communication standards and protocols.

### 3) Application Layer

The application layer is located at the top layer of the IoT network, and it serves as the interface between users and applications. This layer is in charge of retrieving data sent from the network layer and utilizing the collected data for specific operations [59]. As a task of the application layer, it provides the storage facility that can be utilized to store a backup of the acquired data into database. Additionally, this layer predicts the future condition of physical things by analyzing the nature of the received information. From an application perspective, this layer incorporates the functionalities of the IoT framework to develop real-time applications including the healthcare system [60], smart cities [61], smart transportation [62], and smart agriculture [63].

### B. Service-Oriented Architectures

Generally, Service-Oriented Architecture (SOA) is a component model-based framework that connects various functional blocks of applications via interfaces as well as standard protocols [64]. SOA provides viability by allowing software and hardware components to be reused and coordinating the intended services. A new layer named service

layer is added between the network layer and application layer that ensures services are sufficient to assist the application layer extending the three-layer architecture in the SOA framework [65], [66]. As a result, the SOA architecture differs from the conventional three-layer framework by including service layer functionalities. The service layer consists of several components such as service management, service discovery, service composition, and service interfaces [67]. The service management maintains and measures the trust processes in order to fulfill the service's requests. The service discovery unit finds the service's requests. The purpose of service composition is to communicate with the associated things and incorporate services to obtain the requests efficiently. Additionally, all the services are interfaced with one another through service interface unit. The application layer, in general, complies with the user's request for services.

### C. Middleware-based Architectures

The middleware-based architecture is also popular and widely used in the IoT ecosystem nowadays; it is also known as a five-layer architecture. To ensure some of the performance factors like reliability, scalability, and QoS in today's applications, the middleware-based architecture plays a vital role by creating applications efficiently and providing links among the applications, users, and data [68]. The five-layer architecture has been introduced due to the recent developments of IoT and its huge applications in business models. As shown in Figure 3, the five layers include the middleware layer in between the network and application layer as well as the business layer at the top of the layer of the three-layer architecture [69]. The middleware layer aggregates, and filters data retrieved from the hardware, conducts data exploration, and offers access control to the objects for a variety of applications [70]. This layer has grown in importance in recent years since it allows for the growth of

streamlined novel services and the incorporation of existing methods into new designs. The other layer of middleware-based architecture named the business layer organizes the entire services and activities of the IoT infrastructure. This layer takes data from the application layer and creates a business model, graphs, and other representations based on it [71]. This layer is in charge of designing, implementing, and monitoring all IoT components. In addition, the output of the previous four layers is compared with the desired output in this layer to enable the services and user's privacy [72].

## V. IOT PROTOCOLS

Various standards have been introduced to assess the services and relevance that are utilized for IoT solutions to link several things to the Internet in IoT common standards [73], [74]. Although multiple protocols have been developed, they are not all required for a single IoT application at the same time. The IoT protocols for a given application are chosen considering the nature of the application. The most common IoT protocols (depicted in Fig. 4), which are utilized in a variety of applications, are listed below.

### A. Constrained Application Protocol

The Internet Engineer Task Force (IETF), Constrained RESTful Environments (CoRE) research team developed the Constrained Application Protocol (CoAP), which is a Hypertext Transfer Protocol (HTTP) functional and lightweight application layer protocol [75]. As most IoT devices have limited power and storage, the CoAP protocol extends the functionalities of HTTP (which has a relatively high complexity) by fulfilling the needs of IoT devices [76]. This protocol shows how to build a web transfer protocol called REpresentational State Transfer (REST) on the upper level of HTTP. The CoAP uses the User Datagram Protocol (UDP) because it is simple in nature and has a small message size and layout, which helps to decrease the needs of bandwidth, utilize resources, and decrease the overhead of Transmission Control Protocol (TCP) handshaking before data transfer [77]. This protocol has two sub-layers such as the messaging sub-layer and the request/response sub-layer. The first sub-layer (messaging) determines the replications and ensures efficient data transmission over the UDP through exponential backoff as UDP is constrained to error recovery technique. On the contrary, the REST communications are handled by the request/response sub-layer. There are four kinds of messages in CoAP such as confirmable, non-confirmable, reset, and acknowledgment. The CoAP enables efficient delivery, congestion control, and flow control for IoT applications in resource-constrained and unsynchronized objects [78]. The CoAP has several drawbacks, including increased communication delay, packet delivery instability, and the inability to transfer complicated data [79].

### B. Message Queue Telemetry Transport

Message Queue Telemetry Transport (MQTT) is a messaging transport protocol that performs data aggregation of the environmental data and sends it to a web server [80]. This protocol is based on the TCP subscribe and publish messaging model and is intended for lightweight Machine-to-Machine

(M2M), server-to-server, and machine-to-server interactions [81]. Here, the clients are acted as publishers/subscribers and the server is as a broker where the clients are connected to the server through TCP. Generally, the subscriber registers for a particular task in a device, and the data are generated and transferred to subscribers by the publishers through brokers [82]. MQTT is appropriate for utilization in things with limited resources, like those with low power and computing capabilities and are connected to low bandwidth or unstable networks. However, the MQTT protocol is not suited for usage with all forms of IoT applications because it operates over TCP, and the overhead is raised because it uses topic names as texts [83].

### C. Extensible Messaging and Presence Protocol

Extensible messaging and presence protocol (XMPP) is a protocol that ensures low bandwidth communication and short message transfer, making it ideal for video conferencing, publish-subscribe systems, telepresence, multi-party chatting, and talking in IoT [84]. For instant messaging applications, XMPP is appropriate for authentication, security measure, access control, hop-by-hop and end-to-end encryption, and interoperability with various protocols. This protocol serves three functions: client, server, and gateway, and it facilitates two-way communications between any two of these roles [85]. In this scenario, the client connects to the server through TCP protocol and transfers data using the XML streaming standard; the server is in charge for the connection management and routing of the message, and the gateway ensures reliable connectivity among distributed systems. This protocol allows communication among a variety of applications as it is flexible and simple in nature. However, XMPP requires high computing capabilities devices, consumes bandwidth of the network, transfers simple types of data, and is unable to provide QoS [86].

### D. Advanced Message Queuing Protocol

Advanced Message Queuing Protocol (AMQP) is an open platform messaging standard which is utilized at the application level to provide message services such as privacy, queuing, durability, and routing [87]. AMQP ensures reliable and consistent information exchange by using message passing primitives such as one-to-one, one-to-many, and exactly-once delivery. This protocol necessarily needs a stable transport protocol architecture and middleware serves as a gateway between applications and available resources, connecting institutions and mechanisms throughout time and space. The message queue and the exchange queue are two main steps in the AMQP data transmission process. In a message queue paradigm, messages are kept until they are delivered to the recipient. The messages are transmitted in an appropriate sequence in another scenario (exchange queue model) [88]. AMQP also enables the publish/subscribe communication architecture in addition to point-to-point data transfer. There are two kinds of messages found in AMQP like bare messages provided by the sender and annotated messages available at the recipient. However, AMQP requires comparatively higher bandwidth, and it does not guarantee resource discovery [89].

TABLE III  
 IIOT COMMUNICATION PROTOCOLS WITH SOME FUNDAMENTAL FEATURES

Protocol Name	Network Standard	Latest Version (Year)	Transport Protocol	Messaging Model	Architecture	Security and QoS	Application Levels
CoAP	IETF, Eclipse Foundation	RFC 8323 (2018)	UDP	Request/response	Tree	Both	Utility field
MQTT	OASIS, Eclipse Foundations	MQTT version 5.0 (2018)	TCP	Publish/subscribe and request/response	Tree	Both	IoT messaging
XMPP	(RFC 3920-RFC 3923) RFC 4622, RFC 4854, RFC 4979, RFC 6122	XMPP v 1.0.1, XEP-0128 (2019)	TCP	Publish/subscribe and request/response	Client-server	Security	Remote management
AMQP	OASIS, ISO/IEC	AMQP v 2.5.0 (2019)	TCP	Publish/subscribe	P2P	Both	Enterprise integration
DDS	OMG	DDS v.1.4 (2015)	TCP/UDP	Publish/subscribe and request/response	Bus	QoS	Military
LoWPAN	IEEE 802.15.4	6Lo-BLEMesh (2019)	TCP	Publish/subscribe	Star, mesh	Security	Structural monitoring
BLE	802.15.1	6Lo-BLEMesh (2019), MRT-BLE (2018)	TCP/UDP	Publish/subscribe and request/response	Star	Security	Wearable devices
Zigbee	IEEE 802.15.4	Zigbee 3.0 (2018)	UDP	Publish/subscribe and request/response	Star, mesh, hybrid	Security	Consumer electronics

### E. Data Distribution Service

Data Distribution Service (DDS) is a data distribution service protocol based on publish/subscribe model that allows highly dependable M2M, real-time, flexible, and accessible connections [90]. DDS retrieves the edge outliers and gives notifications as well as pushes them to the data analytics engine. The distributed relational information model, which uses a distributed server to keep the application’s specific data, is generated/consumed by the publishers/subscribers. The powerful QoS architecture of DDS is worked based on a series of two principles that provide end-to-end QoS control [91]. DDS allows asynchronous data transfer via a data bus through Peer-to-Peer (P2P) and distribution communication, making it a good fit for IoT applications [92]. As this protocol supports multicasting and broker-less model, it is possible to obtain high reliability and QoS through the use of this protocol.

### F. Low-Power Wireless Personal Area Networks

Low-Power Wireless Personal Area Networks (LoWPAN) are made up of a variety of cost-effective devices that are linked via wireless communication. This protocol has a huge number of applications in IoT architectures due to its small packet sizes, low computing power, low data throughput, and low latency [93]. Additionally, the 6LoWPAN protocol was introduced by incorporating the most recent release of the Internet protocol (IPv6) and LoWPAN. 6LoWPAN makes it easier to maintain the administration process by allowing each constrained object to be accessed independently within the network. Additionally, it is in charge of segmenting and reorganizing IPv6 traffic, guaranteeing unitary routing, reducing protocol stack headers, and providing compliance with the higher levels [94]. This protocol eliminates overall packet overhead as it does not include the extra header information during routing. Besides, 6LoWPAN contains a mesh address header to enable packet routing in a mesh

architecture, but it is unable to provide detailed information of routing to the link layer. 6LoWPAN has various advantages, including ad-hoc self-organization, robust connectivity and standard compatibility, and low power consumption.

### G. Bluetooth Low Energy

Bluetooth Low Energy (BLE), an extended version of Bluetooth offers a small radio with reduced power consumption to operate for a longer period for controlling and monitoring applications [95]. The protocol stack that is utilized in BLE is almost identical to the standard of conventional Bluetooth technology, but it has a larger coverage; approximately 100 meters with low latency [96]. The devices that employ the BLE standard are categorized into two groups: master and slave. The master devices are the ones that play the most important roles and link to slaves. Additionally, the slaves can access and subscribe several master devices. BLE enables devices to investigate as masters or slaves channels in star topology [97]. This technology turns off the radio while idle time and only turns it on to broadcast or receive minimal data packets, resulting in minimal energy consumption. There is a gateway required (another BLE device with network connectivity) for BLE devices while transferring data over the Internet.

### H. Zigbee

Zigbee is a communication standard that ensures reliable, low power, and cost-effective data transfer, but it covers a small range of communication [98]. Zigbee supports star, cluster-tree, and P2P network topologies. A controller, in general, is in charge of the structure and can be found at the middle of a star network, at the root of a tree or cluster architecture, or anywhere else in a P2P topology [99]. There are two stacks in Zigbee standard such as ZigBee and ZigBee Pro; these stacks allow mesh network architectures and to operate with a variety of applications, allowing for low storage and processing power implementations. ZigBee Pro adds new functionalities like a symmetric key in order to ensure

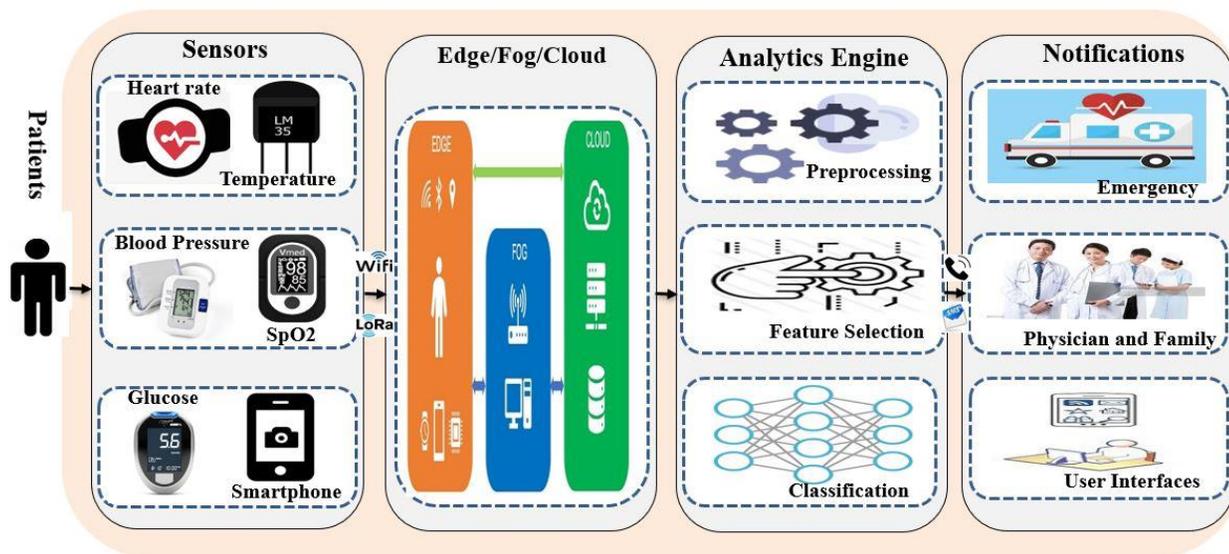


Fig. 5. A general pipeline of IoT-based smart healthcare systems. The sensors (heart rate, temperature, blood pressure, SpO2, glucose, and smartphone) collect the data from the real-time healthcare environment. Some of the data are processed in edge/fog server and the major data analysis occurs in cloud server where the data analytics engines predict the patient status. The emergencies, families, and physicians receive the patient's condition and take further required actions.

security, effective many-to-one relaying for enhanced performance and probabilistic address allocation for flexibility. This protocol offers stringent security and listening mechanisms, making it quite appropriate compared to other wireless communication standards [100]. The Zigbee protocol has a wide range of control and monitoring applications, including smart healthcare, smart homes, industry automation, lighting, and commercial control.

Table III describes the IoT communication protocols with some basic features such as network standard, latest version, used transport protocol, used messaging model, utilized architecture, the security and QoS measures, as well as potential application levels for the protocols that are necessary to compare each of the protocols.

## VI. SMART HEALTHCARE APPLICATIONS

Considering the state of the world today and the disperse of outbreaks and communicable diseases including COVID-19, as well as other things relevant to this global epidemic like massive cost, long distance, and the need for isolation during this crucial timeframe, heading to healthcare institutions is challenging, even sometimes become impossible particularly for the disabled and elderly, who experience severe from at least one chronic illness [101], [102]. As a result, efficient, substantial, and computer-aided technology is very important to address the necessities for long-term care and remote health care monitoring to ensure patients with an adequate quality of life while also reducing the economic strain [103], [104]. IoT has become a revolution for healthcare applications, allowing for the development of predictive and smart systems by linking various IoT devices to perceive real-time bio-physical information from patients including heart rate, blood pressure, glucose level, body temperature, and oxygen saturation level [105], [106]. The most significant contributions of IoT in the healthcare industry are remote patient monitoring, disease

management, preventative care, and assisted living [107], [108]. Additionally, the application environment of IoT for smart healthcare includes hospital management, home healthcare, and e-healthcare/mobile healthcare [109], [110]. A general pipeline of IoT-based smart healthcare systems with the basic components is shown in Fig. 5. Various sensors/medical devices are utilized to collect data from the patient end through the help of healthcare professionals or the patients. The data collection step for healthcare is done in the perception layer and the retrieved data are sent through the network layer using Wi-Fi or LoRa communication technologies. Some portions of the collected data are processed in the edge/fog server to decrease the burden of the cloud server. The main data analytics including preprocessing, feature selection, and classification are done through predictive analytics engines with the use of artificial intelligence techniques; resided in the cloud server. All the processes for the data analysis are performed in the middleware layer. The outcomes of the analytics engines are sent as notifications through call/short messages to the emergencies, physicians and families, as well as interactive user interfaces. The application layer and business layer performed the information consuming step. Although IoT has diverse applications in the healthcare domain, some of the most recent and promising works are described here. The major applications that IoT includes in healthcare domain are depicted Fig. 6.

### A. Biophysical Parameter Monitoring

The monitoring of biophysical parameters is mainly used to observe the changes or absence of changes in the health findings of a patient. The goal of health monitoring is to provide early notification of threatening deterioration by achieving an optimal compromise that included many medical, engineering, and financial design factors. IoT plays a significant role to monitor patients remotely and condensing

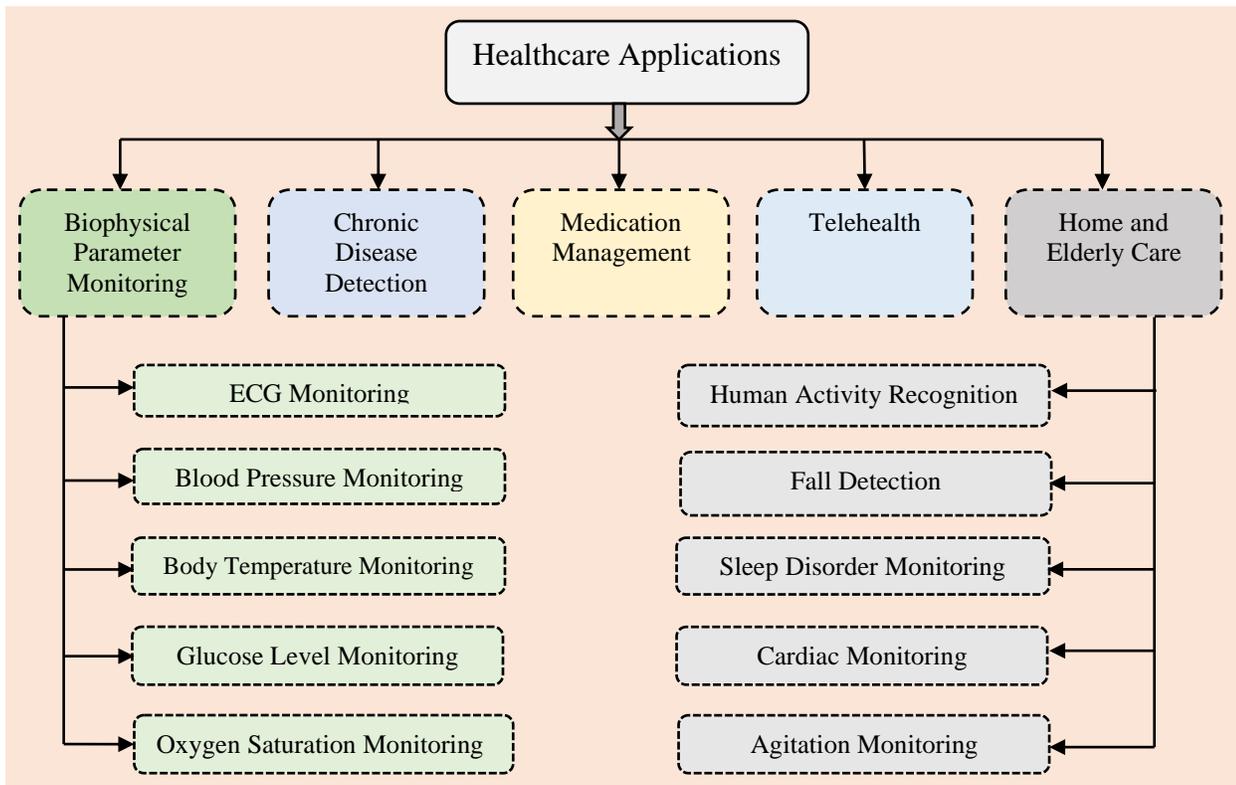


Fig. 6. Major healthcare applications focusing on IoT concepts in the area of biophysical parameter monitoring, chronic disease detection, medication management, telehealth, as well as home and elderly care.

the burden of patients in the hospital as well as decreasing the number of cases. The major bio-physical symptoms of a particular patient involve Electrocardiogram (ECG), blood pressure, temperature, glucose level, and oxygen saturation (SpO<sub>2</sub>). The frameworks that are developed to monitor the above-mentioned parameters of the patients in the IoT environment are described below.

#### (i) ECG Monitoring

Wu et al. [113] introduced a tiny-sized and low-powered ECG monitoring framework that was incorporated into a t-shirt. To collect the ECG signal, the system used biopotential chips. The retrieved data from the patients are transferred to end-users (physicians/families) using Bluetooth. A smartphone application has been developed in this system to visualize the collected data. The minimum power required for the developed system to operate is 5.2 mW. The system is no longer in real-time mode; it is possible to monitor the ECG in real-time by utilizing big data analytics to accommodate larger data capacity. Shaown et al. [114] developed an ECG monitoring system in IoT for ensuring smart health. The developed system used Raspberry Pi, Arduino, ECG sensor (AD8232), and bio pad as hardware components. The collected data are sent to cloud server for processing through Wi-Fi network. The emergency cases of the individuals are automatically sent to doctors to take fast initiatives as a form of an email. The overall accuracy found from the developed system is approximately 80%. In another study, Djelouat et al. [115] presented a wearable ECG monitoring platform that resolved the problems related to power consumption. The device featured a novel design called compressive sensing,

which can reduce power consumption and improve ECG monitoring efficiency. It is shown from the experimental results that the multicore processors are quite appropriate for a gateway-centric solution while maintaining processing capacity and power efficiency. Sahu et al. [116] proposed a cloud-based remote ECG monitoring scheme for cardiovascular patients. The ECG data are transmitted to the AWS through a mobile gateway service. BLE is used as a communication medium between the users and end devices. For data visualization, fast response, and long-live connection, AWS used HTTP and MQTT protocols in this system. Further, Basu et al. [117] introduced a platform for remote patients to monitor their cardiac conditions using the concept of IoT technology. The system used an ECG sensor (AD8232); interfaced with a notch filter (removes the power-line frequencies), and Arduino to process the data initially. The final processing is done using MATLAB tool to remove baseline wander and the processed data are transferred to the cloud as a decision via Wi-Fi that can be accessed by the registered users.

#### (ii) Blood Pressure Monitoring

The measurement of blood pressure (BP) is one of the most important aspects of diagnosing any disorders in the human body. In general, trained professionals measure blood pressure while recording the data of humans. Nowadays, IoT and several sensing modalities are used to measure blood pressure automatically and efficiently. Numerous works [118], [119] have been conducted to make the blood pressure measurement process automated in recent years.

The authors of [120] developed a wearable device to measure systolic and diastolic pressure accurately. The developed system used light-based sensors to collect data and the recorded data are stored in the cloud server to make further analysis. The system was tested with targeted users (more than 70 individuals) and the performance was validated. Singh et al. [121] demonstrated a blood pressure monitoring framework using the concept of IoT, Arduino, and blood pressure sensors. Communication technologies including Bluetooth and Wi-Fi are utilized to transmit data from the patients to the cloud database. The developed system is flexible, cost-effective, compact, and provides the facilities to monitor blood pressure from the home environment. In another study, Hashim et al. [122] introduced a wearable system for blood pressure monitoring in IoT environment. A blood pressure sensor is connected with Raspberry Pi to collect data from the patients. The system is tested with various positions of the patients such as sitting, standing, and lying where the BP value of the sitting position is more correct. The readings of the BP sensor are sent to registered Telegram as well as Gmail application for patient monitoring. In [123], the authors presented the use of machine learning techniques to classify blood pressure in wireless sensor networks environment that can provide BP status and the abnormalities in real-time. In this prototype, a pressure sensor (MPS20N0040D-D) is used for data collection, a microcontroller (ATmega328) is utilized for data processing, and the data transfer is done through a transceiver (NRF24L01). Among the used machine learning techniques, the decision tree algorithm achieved the highest accuracy (97.9%) for BP status detection. Finally, all the data of BP status are visualized in IBM Watson Cloud. Furthermore, Adi and Kitagawa [124] developed an IoT platform for blood pressure monitoring using a tiny embedded device. The used components in this prototype are the pressure sensor, Zigbee Radio Frequency (RF) module, and Raspberry Pi 3. The purpose of the Zigbee module is to send BP data to a database, which is then transferred to an IoT network via Zigbee end-device connection to the Zigbee coordinator. However, the developed system is still working in localhost; not in real-time.

### *(iii) Body Temperature Monitoring*

The body temperature of individuals is a leading determinant of homeostasis maintenance and is used in a variety of diagnostic procedures. In many disorders, maintaining records of temperature changes might help doctors to draw assumptions about a patient's health. The traditional way of temperature measurement is the use of thermometer that takes the records from the different positions of the patient's body such as ear, mouth, or rectum. However, the traditional techniques for body temperature measurement are low comfortable, less flexible, and accurate. In recent days, several frameworks [106], [125] have been developed thanks to IoT technology for human body temperature measurement.

Ota et al. [126] developed a wearable prototype for body temperature measurement that is printed using 3D printer and is applicable to wear on the ear. The developed device records data from the tympanic membrane utilizing an infrared sensor. In this system, a wireless sensor network and data processing

unit are utilized where the prototype is integrated. The environmental conditions and other physical activities could not interfere with the readings of the body temperature. Zakaria et al. [127] proposed a lightweight device for real-time temperature measurement targeting infant patients. The major components of this system include a wearable sensor (LM-35), microcontroller (Arduino), ESP8266, and power module. The collected body temperature is visualized in the cloud server through ThingSpeak and Blynk application. The developed system can provide alert messages to the mediators to take immediate actions while there is a high change of temperature. In another work, Rahimoon et al. [128] introduced a contactless body temperature measurement system to monitor the patients remotely. Two temperature sensors named LM-35 and MLX-90614, Arduino, ESP Wi-Fi shield are used in this prototype. The collected data are transferred to the cloud server for remote access utilizing Wi-Fi connection. However, the developed prototype is quite accurate, real-time, as well as reliable. Boonsong et al. [129] demonstrated a contactless body temperature monitoring platform in IoT environment. The infrared temperature sensor MLX90614 DCI is used here to perceive the data from the environment and sent it to the host computer as well as cloud server using 2.4 GHz microwave frequency. The experimental findings revealed that the developed framework obtained a reliability calibration of 74.7%. Further, Fang et al. [130] used a wearable smart bracelet to monitor the temperature for contact tracing application during the time of the pandemic. The bracelet used RF technology for data collection and the retrieved data are sent to cloud database via wireless technology. However, the system is cost-effective, easy to operate, and provides better data privacy.

### *(iv) Glucose Level Monitoring*

Glucose level monitoring is one of the most significant aspects of managing type 1 or type 2 diabetes. Diabetes is a chronic disease wherein the glucose levels in the body keep going up for an extended time. Fingertyping is the most common method for detecting diabetes, which is validated by blood glucose levels. The development of numerous wearable devices [131], [132] for blood glucose monitoring using modern IoT technologies ensures some features such as comfort, safety, noninvasiveness, and convenience.

Alarcón-Paredes et al. [133] developed a prototype in the shape of a glove that can measure a patient's glucose level and is equipped with a Raspberry Pi camera and visible laser beam. The developed framework used a set of images collected from the patients' fingertips to detect their diabetic status. For data analysis, an artificial neural network is used, and the obtained mean absolute error and Clarke grid error of this system are 10.37% and 90.32% respectively. However, the developed prototype is a little bit bulky to use. Gia et al. [134] introduced an architecture for real-time blood glucose level monitoring in IoT environment. The proposed scheme was designed as an energy-efficient sensor module using nRF communication protocol and developed an energy harvesting unit to extend the battery life of the sensor device. There is a push-button service in the developed prototype that notifies the mediators in the case of abnormal behaviors of glucose like too high or too low. In another research, Rahmat et al.

[135] proposed a prototype named GluQo to monitor the glucose level efficiently. The data from the fingertip are collected using near-infrared LED to determine blood glucose optically and the intensity of the retrieved light calculated the concentration of the glucose of the blood. The glucose level was sent to the mobile application through Wi-Fi signal from the microcontroller. It is found from the experimental findings that the percentage error of the developed prototype is 7.20%. Valenzuela et al. [136] used a double moving average technique enabled by an IoT network to offer a framework for blood glucose monitoring to minimize potential problems in elderly adults. The data for the developed system are collected using a glucometer and this sensor is connected with NodeMCU to make IoT environments. The system can notify doctors and families about a potential critical state in patients at an early stage. Further, the authors of [137] used near-infrared sensors to demonstrate a portable non-invasive glucose monitoring system. The data for the experiments are collected from the fingertip of the patients and the analyzed data are displayed on the Android application. The obtained percentage difference of the reliability test of the developed prototype is less than 25% and the approximate cost is \$15.

#### (v) Oxygen Saturation Monitoring

The measurement of oxygen saturation is a crucial thing in the management and interpretation of the healthcare system. Pulse oximetry is the process of measuring oxygen saturation in a non-invasive way and it is used as a significant factor in the patient care system. The non-invasive techniques for oxygen saturation monitoring solve the problems associated with traditional approaches and ensure real-time monitoring. The integration of IoT-based technologies [138], [139] with pulse oximetry has shown significant potential in the medical field.

Son et al. [140] proposed a SpO<sub>2</sub> monitoring wearable tool that uses IoT technology to give real-time monitoring and prediction of patient health state. The data from the sensor are transferred to cloud database through Internet and this data can be accessed via a web server for the registered users. The experimental findings found that the highest deviation of SpO<sub>2</sub> measurement for this device is approximately 4.4%. It is evident that the prototype is complete, cost-effective, and low-power consumption. The authors of [141] demonstrated a wearable prototype for blood oxygen saturation monitoring from Photoplethysmography (PPG) signal using the concept of Bluetooth low energy. Here, the system introduced a novel adaptive cancellation algorithm using adaptive filtering to remove motion-induced noise. The proposed architecture captured the blood oxygen signals as soon as it received the instruction and sent the data to the mobile phone gateway via Wi-Fi, where it displayed the mathematical waveform. In another research, Zhang et al. [142] proposed a new wearable tool for blood oxygen saturation monitoring that sensed two-channel PPG signals, and sent the signals to the smartphone wirelessly. The dataset for this work is retrieved from the users (eleven individuals) to measure the performance of the proposed framework. It is evident from the experiments that the root mean square error for SpO<sub>2</sub> estimation is 1.8%. However, the performance of the proposed framework is calculated using the data from healthy patients. Adiputra et al.

[143] presented a small, wearable, and cost-effective SpO<sub>2</sub> device in IoT environment for blood oxygen monitoring. To create IoT environment, the developed prototype is connected with NodeMCU which functions as a data processor and Internet network gateway. A dedicated website is developed to ensure online and real-time data accessibility from the cloud. The error rate for SpO<sub>2</sub> monitoring is quite low (1.5% only). Furthermore, Utomo et al. [144] demonstrated a scheme for SpO<sub>2</sub> monitoring using oximeter sensor data through the concept of IoT technology. The data are collected from the finger of the patients in different body positions like standing, sitting, and lying. The sensor is connected with ESP8266 microcontroller, and the collected data are transferred via the built-in Wi-Fi module to the cloud server where the data visualization is done using ThinkSpeak application. The experimental findings revealed that the uncertainty measure of the SpO<sub>2</sub> is 0.04.

#### B. Chronic Disease Detection

Chronic disease is a patient health issue whose consequences are continuous or otherwise lengthy, or an illness that develops over time. Many individuals around the world suffer from chronic illnesses including heart disease, diabetes, asthma, and cancer. In most cases, these illnesses lead to mental health problems, which is one of the most common adverse events of chronic disease. The recent revolution of IoT contributes a lot to develop healthcare frameworks [145], [146] for the people infected with chronic disease.

Shihab et al. [147] developed a system for heart disease detection using the concept of recurrent neural network (RNN) in IoT environment. In this system, an ECG sensor, Arduino, and biomedical patch are used for data collection and to perform the experimental study. The parameters from ECG recordings are retrieved and fed into RNNs with recurrent layers as input. The major advantage of this developed system is that it is quite beneficial for doctors to be able to prescribe medication to patients without having to be physically there. The authors of [148] proposed a IoT-based novel heart disease diagnosis system using machine learning techniques. In the preprocessing step, the noises from the raw ECG signals are removed efficiently ensuring more accurate diagnosis. As hardware components for ensuring IoT platform, the system is comprised of Arduino, ECG sensor, pulse sensor, and temperature sensor. The decision tree algorithm obtained comparatively better performances for heart disease diagnosis using the benchmark dataset. Hebbale et al. [149] presented a non-invasive self-care framework that monitors the blood sugar of diabetes patients using machine learning techniques and IoT. In this system, predictive analytics engines reside on the cloud, and they are used for data analysis for diabetes detection. A smartphone application facilitated the physicians as well as patients to monitor the blood sugar and related risk easily. The decisions from the machine learning approaches are forwarded to the doctors for further analysis and the necessary recommendations from the doctors are sent to the parents through the developed mobile application. Support vector machine obtained the highest accuracy of 82.41% from the experiment. The authors of [150] described an IoT-based diabetes prediction scheme using machine learning

approaches. The data for this system are collected using IoT diabetes sensor. The dataset for the experiment is divided into training and testing set in the percentage of 75% (11,250 records) and 25% (3,750 records) respectively. It is found that the achieved accuracy and error rate of the developed system are 94.23% and 5.77% respectively.

Shah et al. [151] proposed a health parameter monitoring scheme for asthma patients using the concept of IoT and cloud technology. The system utilized a smart sensor to record the respiratory rate of the patients. A watermarking technique ensures data security and authenticity whenever transferred from patients' side to cloud as well as cloud to physicians. A dedicated cloud server is used here to keep the record of the patients and it provides access to mediators for diagnostic and monitoring purposes. The author of [152] demonstrated an architecture to predict asthma using decision tree algorithm in IoT environment. The major components of the developed system are Arduino, ESP8266, GP2Y1010AU0F Optical Dust sensor, LM-35 sensor, and 'NO' Gas sensor. The prototype can notify patients when they need to take pain relievers. It is observed from the experiments that the decision tree algorithm achieved an accuracy of 97.7% for asthma prediction. However, the developed prototype is not fully integrated and bulky. Rehman et al. [153] developed an IoT cancer monitoring framework based on multi-layered architecture that can diagnose and monitor cancer patients remotely. Here, three-layered architectures are utilized which are the patient layer, connectivity layer, and medical layer. The prototype is in the shape of a wristband and can monitor the basic health issues of cancer patients. The major advantage of this architecture includes it gives continuous monitoring of the patients that is helpful for the physicians to generate a complete history of the patients which in turn would be helpful for treatment in the later stages. In [154], the authors demonstrated various types of architectures and frameworks to develop IoT-based healthcare platforms targeting cancer patients. For communication purposes, a wireless sensor network is developed that can accommodate a high number of sensors and the data analysis is done on the cloud server. The security measures and operational challenges regarding the IoT healthcare system for cancer patients are also described here.

### *C. Medication Management*

Smart medication is one of the most significant concerns in the IoT-based smart healthcare application. It is very critical as it is intrinsically related to human health, and missing a dose of medication can have serious effects. Medication nonadherence is particularly common in older individuals as they age and eventually increases the chance of diseases including dementia, and cognitive decline. Hence, it is badly needed for them to use assistive technologies to keep the track of medication timing and dose. In recent times, several studies [155], [156] have been performed emphasizing on employing IoT technology to track patients' medication adherence.

Bharadwaj et al. [157] developed an IoT device in the shape of a medical box to remind the patients in the time of medication. In this prototype, there are three trays to keep the medicine for three different periods such as morning, noon, and evening. The data are stored on the cloud server and

smartphone application retrieved the data from the cloud and used it to remind the patients for medication. Srinivaset al. [158] introduced a home-based medicine box named iMedBox to manage medicine for patients in IoT environment. The used sensors in this prototype notified the patients via a wireless connection and an Android application to take their medications on time and to keep in closer contact with their doctors. In another research, Latif et al. [159] presented a wearable IoT device called I-CARES to diagnose health issues and medication for elder patients. The system described an algorithm for data analysis and aided the medical professionals to make decisions for early-stage treatment of predicted diseases or illnesses. Additionally, the developed prototype can predict emergencies and call emergency personnel when necessary. Tsai et al. [160] demonstrated an intelligent pillbox for the older individual and nursing home needs using the concept of electronic technology and network functionality. Using embedded sensors, the developed device detects the signal when patients take their medications and displays the schedules and deadlines as text, pattern, or voice on the LCD screen. The hardware unit is made up of webduino for data transmission and can interact with a web server via the IoT architecture. The sensed data are transferred to the Arduino module, which is then sent to the developed pillbox, allowing the elderly to maintain their medications. The authors of [161] designed a smart medication box for ensuring medication monitoring in IoT platform. The prototype includes six distinct parts to keep track of six different pills, and it can send timely reminders to the caregivers/patients through the smartphone. A simple authentication process is developed to avoid overdosage and improper intake of medicines. In addition, the system is able to provide monitoring facilities of temperature and heartbeat through the use of biosensors. Vardhini et al. [162] proposed an assistive system to help elderly people with memory impairment for keeping track of their medication schedules and inform them to consider taking their medicines at the appropriate times. The main hardware components for the prototype include NodeMCU, LDR sensor, motor, switch, power supply (battery), LCD monitor, and buzzer. The developed system is low-cost (approximately \$15), and easy to use. However, the system has not tested in any hospital environments.

### *D. Telehealth*

Telehealth is the use of technologies such as digital devices, smartphone apps, and webpages to instruct, detect, and even prescribe remedy to individuals suffering from health problems. It primarily allows individuals of all ages to be monitored remotely. The telehealth system monitors the significant clinical data and takes oversight of the individual's well-being. Numerous frameworks [163], [164] have been done to ensure telehealth services using IoT technology in recent times.

Rokonuzzaman et al. [165] developed a telehealth platform based on the IoT concept to create warnings automatically for providing individuals with desirable healthcare under constant health contexts. A smartphone application called 'village doctor app (VDA)' is deployed for real-time monitoring. This scheme provides the monitoring facilities of heart rate and

temperature. The hardware components of the developed prototype are heart rate sensor, temperature sensor, Arduino, NodeMCU, battery, and LCD display. The physicians can access the data from the cloud server through VDA application. Ganesh et al. [166] introduced a framework named 'AutoImpilo' to improve the telemedicine and telehealth services in IoT networks. The designed approach ensured that all online medical checks were conducted in collaboration with consulting the doctors or specialists. This system is quite beneficial for individuals who are unable to go outside due to ages or quarantine issues. The system used a smart card in the authentication step to ensure privacy, but it is not linked to the cloud. In another work, Tsiouris et al. [167] integrated many online technologies and compatible components into a unified framework for digital coaching, encouragement, and empowerment of elderly with balance problems. This approach has been proven in a telerehabilitation system for individuals with balance issues that uses augmented reality to provide a surrogate physiotherapist as a superimposed hologram, along with easy-to-use wearable sensors. Hewa et al. [168] employed many decentralized applications to transmit cryptocurrency to patients' wallets effectively and reliably as an incentive for providing their health information utilizing edge computing and blockchain technology. To provide scalability with a large number of connected biomedical sensors to the cloud, the system included memory offloading functionality into the blockchain. The proposed platform is tested in a near real-world setting employing the Hyperledger Fabric blockchain infrastructure and Raspberry Pi modules to imitate smart sensor activities. Further, Hamil et al. [169] described a telehealth platform for bio-signal diagnosis and classification using e-health sensors data considering IoT environment. The Arduino and Raspberry Pi with sensors are used for data acquisition and processing. The used sensors are here ECG sensors, body temperature sensor, SpO2, position sensor, airflow sensor, and galvanic skin sensor. Various machine learning algorithms are tested with PhysioNet databases where the best accuracy of 99.56% is found from convolutional neural network-support vector machine for atrial fibrillation classification.

### *E. Home and Elderly Care*

Elders can continue living at home freely with the assistance of smart home care services, as IoT devices provide them with the security of being observed and the capability to instantly call for help in the case of an emergency. Modern IoT technologies, as well as relevant wearables devices, are frequently utilized in ambient assisted living environments to monitor older patients who are unable to move rapidly and need longer time to reach clinics for routine or urgent medical facilities [170], [171].

Abdelgawad et al. [172] proposed a system for health monitoring of older people in an ambient assisted living environment where the data are retrieved from several sensors and transferred it to the cloud server for further investigation. The prototype incorporates six different sensors, Raspberry Pi, Wi-Fi module, cloud server, sensor interface circuits, and an indoor positioning module enabled by Bluetooth low energy. A feedback signal is sent to the users based on the behavior of

the data so that they could take necessary actions in the case of emergencies. The authors of [173] developed a wearable framework for health data monitoring (stress, blood pressure, and position of the users) for the elderly in smart home environments. The stress of the elders is detected using electrodermal activity, PPG, and skin temperature sensors. The blood pressure is estimated utilizing the data from the PPG sensor. The location of the individuals is detected using a voice-assisted indoor location module. The highest accuracy of 94% is obtained from the combination of multiple signals for stress detection. Finally, a prototype is developed to test the location detection system in a smart home environment. In another work, Debauchea et al. [174] demonstrated a novel architecture for elderly psychological signals monitoring utilizing the concept of IoT and fog computing. The framework includes a wireless sensor network consisting of various psychological and environmental signals, a local gateway for local and fast storage, and Lamda cloud server for data processing as well as storage. The main advantage of this architecture is that it can provide local gateway monitoring of new and current patient data. The latency and CPU usage of the fog architecture is 7 ms and 7.86% respectively. In [175], the authors presented a novel and scalable platform for smart home and elderly care based on IoT concept. The system employed various sensors data such as heartbeat, pressure, and gas sensor for patients as well as smart home monitoring through the use of Raspberry Pi and cloud server. The medications are suggested by the registered doctors based on the health conditions of the patients which are delivered through wireless sensor networks in the form of texts or email. The experimental findings revealed that the mobility absorption of the designed network is approximately 90%. However, a few numbers of signals are considered here for health and home monitoring. Furthermore, Srinivasan et al. [176] used the concept of IoT and machine learning to develop an elder care system. The prototype of this framework contains sensors connected to an ESP32 and a home module with an IoT camera attached to a Raspberry Pi. The biophysical parameters are retrieved through sensors and processed in the AWS cloud utilizing machine learning approaches. The warnings are directed to caregivers automatically in the case of abnormalities. The locations are tracked through a GPS module that are transferred to the mediators to let them the location of the individual patient. All the data for the experiments are visualized through the developed smartphone application.

## VII. OPEN CHALLENGES AND FUTURE TRENDS

Internet of Things and the technology and research state related to it are in their nascent state compared to other networking research topics. The state-of-the-art connection models and architectures are recently being developed. IoT in general and IoT in healthcare in specific still face many challenges. Understanding and exploring these challenges such as the security and privacy risks, lack of standardization, big data management, and costs are imperative to realize the full potential of Internet of Things in industrial, healthcare, and personal use cases among other promising domains. The major challenges and the potentials future directions for IoT

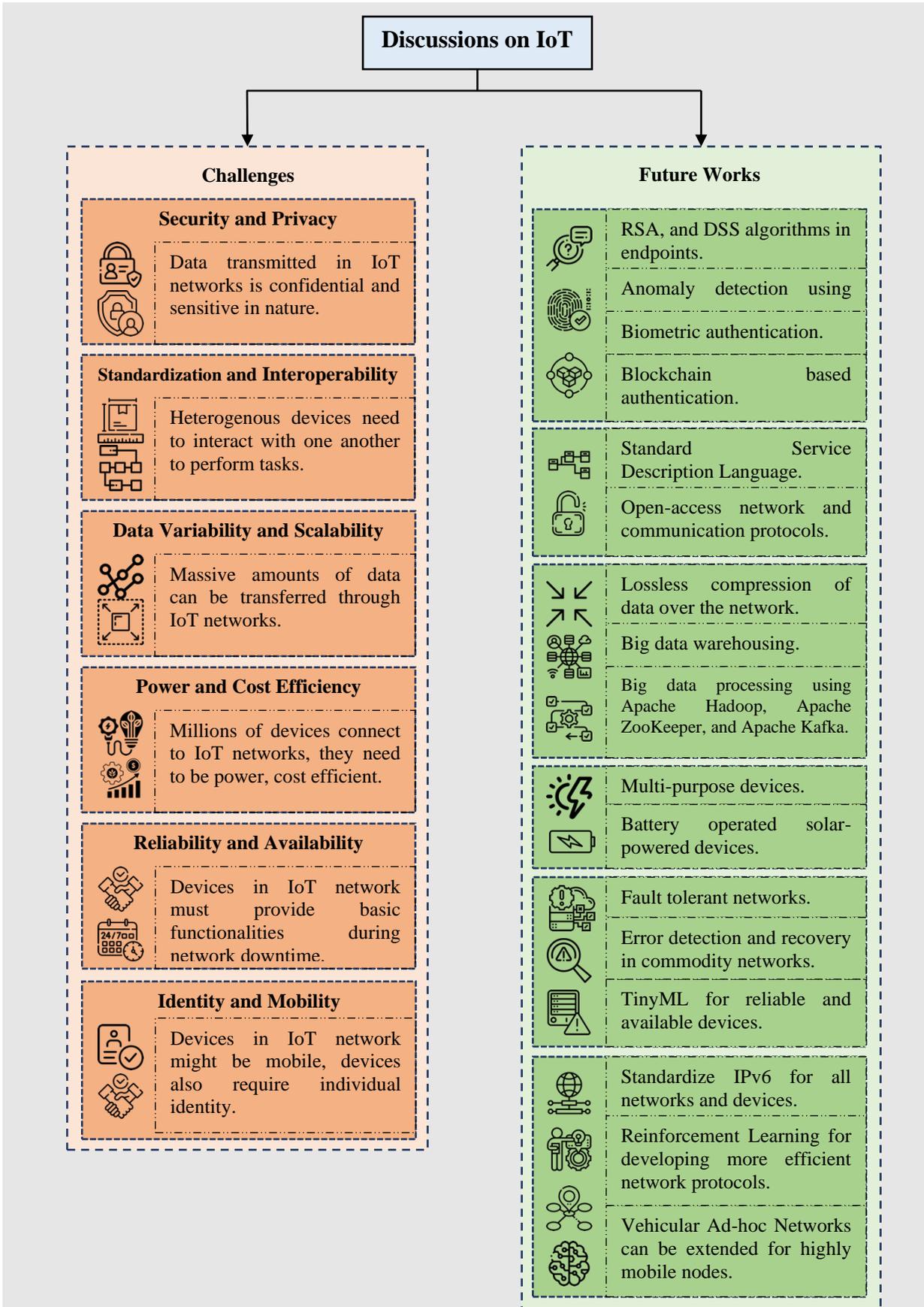


Fig. 7. Challenges and future research directions of IoT. The major challenges encompass security, reliability, scalability, availability, and cost-efficiency. The potential future directions include the area of blockchain, TinyML, reinforcement learning, and big data processing.

research are illustrated in Fig. 7 in brief. The open issues, as well as future research trends related to IoT, are discussed as follows.

### *A. Security and Privacy in IoT*

Security is a huge concern in any networked system. IoT is a collection of devices connected via a single network or multiple networks. Thus, the security issues concerning networked systems are also relevant to IoT systems [177]–[179]. Devices in IoT are also heterogeneous in nature—which adds to the complexity in maintaining the security of the transmitted data. To provide complete security, all of the types of devices connected to IoT networks, would need to be completely secure—which is a near impossible task. Security can be breached on both hardware and software levels. Modern smartphones often have exotic zero-click exploits, meaning the devices can be hacked without any action by the user of the device. Modern operating systems – be it for desktop or smartphones often have zero-day exploits, meaning the devices running these updated operating systems can be exploited by hackers even on the first day of the update. Exploited devices can act as Byzantine nodes in IoT networks, making the entire network vulnerable and stealing data from other devices. Especially in healthcare systems, the underlying data is extremely sensitive and confidential in nature. Healthcare data not only contain health-related information but also contains identifying information of the patients including social security numbers, social insurance number, and insurance information. Any leak or compromise in such networks might result in catastrophic ramifications for the patient such as identity theft, and customized scamming. Improving the security and privacy of data in healthcare systems is a research challenge.

In the future, cryptosecurity algorithms such as the RSA encryption algorithm, Digital Signature Standard (DSS), and ElGamal can be utilized in all endpoints in IoT networks to provide security. Secure hash algorithms can be utilized to ensure data integrity. Blockchain technology can be leveraged to reduce man-in-the-middle and network eavesdropping attacks [180], [181]. Non-Fungible Token (NFT) technology can save patients from counterfeit products or services. NFTs can also help patients to decentralize their sensitive data and to share healthcare data while keeping their identities anonymous. Biometric authentication techniques such as fingerprints, voice recognition, face recognition, and iris recognition as well as software-based authentication such as two-factor authentication, access cards, and seed phrases should also be standardized in the future for systems connected in IoT networks. Artificial intelligence-based approaches for anomaly detection in networks should be explored in the future for improving security. Due to advances in TinyML [182], it might be possible to run anomaly detection models in the future in resource-constrained devices [183]. These would greatly improve the security and privacy of the users and the transmitted data.

### *B. Standardization in IoT*

Heterogenous types of devices are interconnected via complicated networks in an IoT environment. Each of these devices might use distinct architectures or protocols for

generating or transmitting data. The devices are also different from software and hardware perspectives. The management of such devices including the collaboration of the devices in a software or hardware level, proper addressing, marshalling, de-marshalling, optimization at a protocol or architectural level, and identification is a huge research challenge. Measures should be taken to draft and standardize IoT architecture and network protocols in the future [184].

### *C. Data Variability in IoT*

Data in Internet of Things can vary in type, size, and formation. Due to the sheer number of connected devices in IoT networks, storing the data in solutions such as in conventional RAID systems or conventional databases is very inefficient. Huge volumes of data are generated in a very short period in IoT networks. Conventional database systems are not capable of storing or efficiently retrieving them. Management of the huge volume of data such as handling spatial or temporal information, handling differing data sizes, and handling different types are massive research challenges. Devices in healthcare systems transmit data in various formats such as 2D image formats, 3D imaging formats, and numerical sensor readings in time-series format.

Big data warehousing and processing frameworks such as Apache Hadoop, Apache ZooKeeper, and Apache Kafka can be utilized to efficiently deal with the huge volume of data in the future [185]–[188]. Some of these frameworks also provide error detection and error recovery of the stored data, which will help in persisting historical data. Some of these frameworks are also capable of dealing with multiple types of data at the same time. These frameworks are also highly cost and space-efficient. Lossless compression models can also be researched to transmit huge volumes of data over IoT networks [189].

### *D. Identity in IoT Networks*

IoT networks generally consist of a huge number of devices. Every device needs a unique identity in the network. The most used core protocol in standard-based interconnecting networks is IPv4. The IPv4 protocol uses 32 bits to represent unique addresses which provide a maximum of  $2^{32}$  address spaces. IPv4 addresses are represented in 4 numbers separated by 4 dots. Due to the huge number of devices connected to IoT networks, it is possible to run out of address space. Healthcare systems have multiple monitoring systems per person. For a sufficiently large elderly population in a single network, the address space for all devices might be insufficient. While a lot of devices support IPv6 nowadays, developing more lightweight and robust solutions for addressing the identified problem is a research challenge.

In the future, IPv6 protocol can be standardized for all IoT networks [190], [191]. IPv6 addresses are represented as eight groups of numbers. Each group contains four hexadecimal digits. The address space of IPv6 is  $2^{128}$  which is suitable for addressing the huge number of devices in IoT networks. IPv6 also supports shorthand representation and compression of network addresses, which reduces total used bandwidth over the network.

### *E. Lack of Service Description Language*

A service description language is a special form of Interface Description Language that is used for describing a particular service. Interface description languages enable programs to interact with one another regardless of origin or language. Similarly, service description language enables services from varying devices and software/hardware combinations to interact with one another. Due to lack of standardization, devices in IoT networks use vastly different protocols, architectures, and data types. The underlying service routines dealing with these differences are also vastly different from one another. A unified service description language would greatly benefit IoT networks by enabling seamless collaboration and interoperability among devices. Creating a unified service description language is a massive research challenge. In the future, service description languages such as XML, and UML, can be extended to create a standardized service description language for IoT networks. Research should also be focused on developing specialized service description language for IoT networks [192], [193].

### *F. Design of Service-Oriented Architecture*

Service-Oriented architecture is a style of software architecture where components of an application interact with other components of that application or other application via services through utilizing a communication protocol over a network. The connection is independent of vendor or other limiting hardware or software technologies. The design of service-oriented architecture for IoT systems is a huge challenge. On one hand, service-oriented architecture simplifies the management of heterogeneous types of connected devices. On the other hand, service-oriented architecture introduces additional overhead to devices. Most IoT devices are resource-constrained. Adding overhead to these resource-constrained devices slows down the entire network making data processing, collection, and transferring more difficult. Thus, researching lightweight service-oriented architecture with minimum overhead that facilitates big data warehousing and processing is a huge research challenge [194]–[196]. In the future, novel architectures for IoT networks should be developed to be modular and service-oriented in nature.

### *G. Hardware Customization*

IoT networks currently degenerate into traditional ICT oriented networks. Similarly, the hardware of various intelligent devices is not customized to specific protocols. IoT devices generate huge amounts of data within short amounts of time. Higher bandwidth networks are necessary alongside big data measures to store and process the data in real-time. Developing novel methods to transport the huge amounts of data in commodity networks is a huge research challenge, as it is impossible to deploy high bandwidth high-frequency networks all around us. Similarly, optimizing the hardware of general intelligent things to efficiently use certain universal IoT protocols is a research challenge.

In healthcare systems, various sensors are used to monitor patients. Developing novel hardware design solutions to contain various sensors in small housing would enable a single device to monitor various aspects of a patient. In the future,

various bio-inspired optimization techniques such as swarm optimization, and genetic algorithms should be utilized to automatically develop optimized hardware design for various use cases.

### *H. Mobility of IoT Devices*

In an interconnected world from a network perspective, intelligent devices are expected to disconnect from one network and connect to other networks. In traditional networks, mobility is a huge issue. For mobile nodes, routing tables have to be re-calculated each time nodes move out of range from one another and come into the range of other nodes. This calculation puts a huge overhead on the entire network when numerous nodes with high mobility are present [197]. Modeling and handling highly mobile nodes in IoT networks are a huge research challenge. In healthcare systems, some monitoring devices might be mobile in nature, while others might be stationary. For example, wearable monitoring devices might be highly mobile, while surveillance monitoring devices would be stationary. Patients would wear and bring the highly mobile monitoring devices to their activities of daily life. Thus, optimizing the various aspects of these mobile devices, such as route discovery, routing table generation, efficient data transfer, and reducing data costs is a research challenge.

In the future, artificial intelligence-based approaches such as reinforcement learning-based techniques can be used to develop networks facilitating highly mobile devices [198], [199]. Vehicular Ad-hoc Network (VANET) architectures can be extended in the future to IoT networks involving highly mobile nodes [200].

### *I. Reliability in IoT Networks*

Reliability is a huge issue in commodity networks. Regardless of network and type of protocol, network packets get lost with the data. While some data warehousing solutions provide checkpointing and state management for error detection and recovery, it is not the norm and requires extensive installation and support. Developing lightweight reliable networks with error detection and error recovery is a huge challenge. Devices connected in IoT networks themselves need to be reliable [201]–[203]. Erroneous reporting might result in faulty directions from central controller servers. Healthcare systems in general require reliable and fast networks. Any drop in data, as well as monitoring results, might be irreversibly harmful for the users. For example, in stroke, diabetes, Alzheimer's, or fall monitoring systems, it is imperative to monitor the patients without interruptions, and any kind of delays in transmission or monitoring might prove fatal for the patients. Developing specialty fault tolerant and state-recovery-capable networks for healthcare systems is a challenge. Similarly, unreliable devices in healthcare IoT networks can result in the loss of life of patients in extreme cases.

In the future, network traffic forecasting models should be developed to predict traffic load and allocate network resources accordingly. Various checkpointing algorithms can be used for error detection and correction in networks. Network designs should also be fault tolerant. Advances in TinyML enable us to deploy and run machine learning models

**TABLE IV**  
SUMMARY OF CHALLENGES IN LARGE-SCALE DEPLOYMENT OF IOT NETWORKS AND FUTURE RESEARCH RECOMMENDATIONS

Type	Concerns	Recommendations
Security and Privacy	<ul style="list-style-type: none"> <li>▪ Healthcare data is highly sensitive and contains personal identifying information such as social security information, and insurance information.</li> </ul>	<ul style="list-style-type: none"> <li>▪ More secure overlay networks such as The Onion Router (TOR) network might be used to transfer confidential data.</li> <li>▪ Technologies such as blockchain, and NFT tickets can be used to provide authentic and customized service.</li> <li>▪ Existing security solutions such as RSA, seed phrases, and DSS might be employed in all connection endpoints.</li> <li>▪ Authentication and identity verification methods such as password, fingerprint scanning, signature, voice pattern, and smart card can be employed in application protocols.</li> <li>▪ Artificial intelligence-based approaches can be used to detect anomalies in IoT networks.</li> </ul>
Standardization and Interoperability	<ul style="list-style-type: none"> <li>▪ Different devices in IoT networks use differing application protocols, data representation methods, network protocols, marshalling, de-marshalling, and identification.</li> <li>▪ No standard service description language.</li> <li>▪ Limited interoperability among devices.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Developing a standardized service description language would benefit the standardization and interoperability of IoT devices.</li> <li>▪ Open-source implementations of vendor-locked applications and networking protocols would enable interoperability.</li> <li>▪ Standardizing application and networking protocols would simplify interoperation among devices in IoT networks.</li> </ul>
Data Variability and Scalability	<ul style="list-style-type: none"> <li>▪ Data transmitted in IoT networks vary by size, type, and representation over network.</li> <li>▪ Massive amounts of data can be transmitted over an IoT network in a very short amount of time.</li> <li>▪ General applications and networks are not scalable in nature.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Utilizing big data warehousing techniques and open-access application frameworks such as Apache Hadoop, and Apache zookeeper will allow the storing and processing of huge amounts of data.</li> <li>▪ Modularity can be prioritized to make devices in IoT networks more scalable.</li> <li>▪ Lightweight service-oriented architecture of devices would enable scalable big data warehousing and processing.</li> <li>▪ Utilizing available SaaS, PaaS, and DaaS platforms such as AWS, Google App engine would increase the scalability of IoT-orientated solutions.</li> <li>▪ Lossless compression algorithms might be utilized to transmit huge volumes of data over standard IoT networks.</li> </ul>
Power and Cost Efficiency	<ul style="list-style-type: none"> <li>▪ Increasing number of intelligent devices connected in IoT networks has harmful effects on nature.</li> <li>▪ Devices are not as power-efficient as they could be.</li> <li>▪ Setting up and maintaining all-day monitoring via multiple devices is not cost-efficient.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Solar-powered hardware solutions would increase the sustainability and eco-friendliness of the huge number of devices used in IoT networks.</li> <li>▪ Creating multi-purpose generalized devices would reduce the number of separate devices necessary to monitor or surveil patients or environment. This reduction in number would also reduce the overall cost.</li> <li>▪ Specialized hardware for task-specific purposes might reduce overall power consumption.</li> <li>▪ Optimized software would also reduce the amount of necessary processing, which might optimize power consumption.</li> </ul>
Reliability and Availability	<ul style="list-style-type: none"> <li>▪ Devices used in monitoring purposes in both industrial and healthcare use cases need to be available all the time regardless of network or other failures for avoiding dangerous or life-threatening situations.</li> <li>▪ Intelligent devices used for monitoring and surveillance purposes need to be reliable at all times. Unreliable monitoring can result in erroneous diagnoses which might even lead to death of patients.</li> <li>▪ IoT networks need to maximize availability and reliability. Downtime of networks might lead to loss of valuable data.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Fault-tolerant development principles should be followed while developing specialized IoT networks.</li> <li>▪ Error detection and recovery techniques in networking such as distributed checkpointing, and coordinated checkpointing can be implemented to increase network reliability.</li> <li>▪ Network traffic analysis and traffic forecasting might be used to anticipate network load, which will help in allocating appropriate resources to increase network availability.</li> <li>▪ Simplified versions of applications must be available in devices to facilitate basic services even during network failure or downtime.</li> <li>▪ TinyML deployment techniques can be leveraged to ensure minimal functionality during network downtime.</li> <li>▪ Sensing modules in devices must be within standardized error tolerance limits and must undergo scheduled testing to guarantee utmost reliability.</li> <li>▪ Using state-of-the-art battery technologies might improve the reliability and availability of devices.</li> </ul>
Identity and Mobility	<ul style="list-style-type: none"> <li>▪ IPv4 network protocol might not be sufficient to address millions of devices connected in IoT networks.</li> <li>▪ Networks and routing protocols are not efficient in dealing with numerous highly mobile devices in IoT networks.</li> </ul>	<ul style="list-style-type: none"> <li>▪ IPv6 can be adopted as the standard Internet protocol for IoT networks.</li> <li>▪ Artificial intelligence approaches such as reinforcement learning techniques can be utilized to develop and test new routing protocols capable of efficiently dealing with highly mobile nodes.</li> <li>▪ Vehicular Ad-hoc Networks already provide networking solutions for mobile and stationary nodes in networks. Relevant components from VANETs can be evolved for use in IoT networks.</li> </ul>

in resource-constrained environments. In the future, devices connected in IoT networks should use TinyML to run basic models to provide basic service functionalities during network downtime or other failures. This would increase the reliability factor of the devices. To reduce the downtime of the devices, advanced battery solutions should be used in the future.

### J. Scalability in IoT Networks

IoT networks might have millions or billions of interconnected nodes. General networks and services are not scalable in nature. Scalability is a huge challenge for such IoT networks [204], [205]. In healthcare systems, each patient might have multiple types of monitoring going on at the same time. For example, elderly patients might be monitored for

heart diseases, glucose levels, diabetes, Parkinson's, Alzheimer's, and falls at the same time. For a sufficiently large elderly population, the number of these systems would reach millions, requiring specialty scalable services and applications.

In the future, the potential of using existing Database-as-a-Service (DaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) to increase the scalability of IoT services and networks should be explored. The research focus should be on developing modular IoT solutions that can scale on need.

#### *K. Availability in IoT Networks*

IoT has applications in industrial and healthcare domains among other potential application areas. Industrial devices are placed for continuous monitoring of various parameters such as temperature, humidity levels, and pressure. Even during network failures, the devices should be able to provide basic monitoring services to avoid catastrophic failures in industrial cases. In the healthcare space, monitoring devices need to be available at all times similar to industrial use cases. Lack of availability might result in serious bodily harm or even death. Devices in IoT networks must provide basic monitoring and action services even when they are disconnected from networks or when network failures happen. The availability should be implemented in both hardware and software levels.

Similar to the reliability, research should be focused on deploying basic models into devices using TinyML, which would increase overall availability. Novel error detection and error correction in fault tolerant networks should be explored to increase the availability of the network.

#### *L. Interoperability in IoT Networks*

Interoperable applications and services can communicate and transmit data among themselves regardless of hardware or software differences. However, interoperability is very hard to achieve. New protocols or architectures that are constantly being developed do not always support all legacy protocols and architectures, making data transmission and interaction between devices very complex and problematic. Similarly, operating systems and various applications also have different implementations, making data sharing very difficult. Vendors often-time have patented and exclusive implementations that make their devices only compatible with other devices of the same vendor. Thus, interoperability is a huge research challenge for IoT [206], [207]. Interoperability is very important in healthcare systems as various medical equipment have differing hardware, protocol implementations, and data representation. For a smooth deployment and operation of IoT networks in the healthcare sector, the various devices and services need to be interoperable.

In the future, the research focus should be on developing open-access network architecture and protocols to facilitate interoperability among devices. Open-access implementations of specialty architecture and protocols would also facilitate this issue.

#### *M. Power and Cost Efficiency in IoT Networks*

IoT networks have millions of nodes. Power and cost are huge concerns for such a huge number of devices. The entire

world is also experiencing various global natural catastrophes due to global warming and climate change caused by extracting and depending on fossil fuels, trashing the oceans with electronic waste, and chemical waste. With an increased understanding of the causes behind the sudden climate change and global warming, researchers are increasingly moving towards sustainable, eco-friendly, and bio-degradable solutions. Making IoT devices more eco-friendly, cost-efficient, and power-efficient is a massive research challenge [208]. Similarly, converting medical intelligent monitoring devices in healthcare IoT networks into more multi-purpose, power and cost-efficient, long-lasting, eco-friendly versions is a research challenge.

In the future, research should be focused on simplifying and combining multiple sensing modalities in single devices to reduce the number of total sensors necessary to monitor and surveil users. The focus should also be on developing more area-surveillance solutions. Area-surveillance technologies would reduce the number of devices per individual. Reducing the total number of devices needed per user would also drastically reduce the cost to effectively deploy an IoT solution. In the future, research should be focused on transforming commodity devices into solar-powered versions. Research on hardware and software optimization would also increase the power the efficiency of devices. Making the devices solar-powered would reduce the overall pressure on fossil fuel, which has beneficial effects on nature.

The summary of challenges in large-scale deployment of IoT networks and future research recommendations are shown in Table IV to provide a broad idea to the readers in a short look.

## VIII. CONCLUSION

The Internet has significantly shaped the way people live, allowing individuals to interact with one another on a virtual level in a variety of situations ranging from professional to social. The Internet of Things could contribute meaningfully to this system by enabling communication among connected devices, which tends to result in the dream of “anymedia, anytime, anything, anywhere” connectivity. This paper focuses on the cutting-edge IoT device capabilities, architectures, and protocols that describe the IoT conceptual framework. The IoT device capabilities for hardware and software tools are thoroughly demonstrated in this paper. There have been discussions about possible IoT architectures, such as the conventional three-layer architecture, the SoA based architecture, and the middleware-based architecture. Additionally, the IoT communications protocols with their distinguished features are incorporated briefly in this paper. We have highlighted various IoT applications for smart healthcare that have been developed in the recent decades to ensure some facilities for medical practitioners such as monitoring and identifying a variety of health problems, measuring various health factors, and offering diagnosis and treatment at remote locations. Lastly, the current challenges and gaps related to the development of IoT-based healthcare applications, along with future improvement and research focus in the coming years have been explored here. Hopefully, this paper will provide a stable platform for scholars and

scientists willing to engage in learning more about IoT technologies in the context to fully grasp the general architecture and roles of the multiple elements and processes that comprise the concept of Internet of Things.

## APPENDIX

TABLE A  
LIST OF ABBREVIATIONS

Abbreviation	Definition	Terminology
ADC	Analog to Digital Converter	General
AI	Artificial Intelligence	General
AMQP	Advanced Message Queuing Protocol	Technical
AWS	Amazon Web Services	General
BLE	Bluetooth Low Energy	Technical
BP	Blood Pressure	Medical
CoAP	Constrained Application Protocol	Technical
CoRE	Constrained RESTful Environments	Technical
CPU	Central Processing Unit	General
DaaS	Database-as-a-service	Technical
DDS	Data Distribution Service	Technical
DSS	Digital Signature Standard	Technical
ECG	Electrocardiogram	Medical
GPIO	General Purpose Input Output	Technical
GPS	Global Positioning System	General
HTTP	Hypertext Transfer Protocol	Technical
IETF	Internet Engineer Task Force	General
I/O	Input/Output	General
IPv6	Internet Protocol Version 6	Technical
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission	General
IoT	Internet of Things	Technical
LoWPAN	Low-Power Wireless Personal Area Networks	Technical
ML	Machine Learning	General
M2M	Machine to Machine	Technical
MQTT	Message Queue Telemetry Transport	Technical
NFT	Non-Fungible Token	Technical

## REFERENCES

[1] Y. Song, F. R. Yu, L. Zhou, X. Yang, and Z. He, "Applications of the Internet of Things (IoT) in Smart Logistics: A Comprehensive Survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4250–4274, Mar. 2021.

[2] D. C. Nguyen *et al.*, "6G Internet of Things: A Comprehensive Survey," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 359–383, 1 Jan. 2022.

[3] F. Guo, F. R. Yu, H. Zhang, X. Li, H. Ji and V. C. M. Leung, "Enabling Massive IoT Toward 6G: A Comprehensive Survey," *IEEE Internet Things J.*, vol. 8, no. 15, pp. 11891–11915, 1 Aug. 1, 2021.

[4] L. Chettri and R. Bera, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16–32, Jan. 2020.

[5] M. Nasr, M. M. Islam, S. Shehata, F. Karray, and Y. Quintana, "Smart Healthcare in the Age of AI: Recent Advances, Challenges, and Future Prospects," *IEEE Access*, vol. 9, pp. 145248–145270, 2021.

[6] F. John Dian, R. Vahidnia, and A. Rahmati, "Wearables and the Internet of Things (IoT), Applications, Opportunities, and Challenges: A Survey," *IEEE Access*, vol. 8, pp. 69200–69211, 2020.

[7] P. Asghari, A. M. Rahmani, and H. H. S. Javadi, "Internet of Things applications: A systematic review," *Comput. Networks*, vol. 148, pp. 241–261, Jan. 2019.

[8] G. Marques, R. Pitarna, N. M. Garcia, and N. Pombo, "Internet of Things Architectures, Technologies, Applications, Challenges, and Future Directions for Enhanced Living Environments and Healthcare Systems: A Review," *Electronics*, vol. 8, no. 10, p. 1081, Sep. 2019.

[9] F. Alshehri and G. Muhammad, "A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare," *IEEE Access*, vol. 9, pp. 3660–3678, 2021.

[10] S. Ketu and P. K. Mishra, "Internet of Healthcare Things: A contemporary survey," *Journal of Network and Computer Applications*. 2021.

[11] M. M. Dhanvijay and S. C. Patil, "Internet of Things: A survey of enabling technologies in healthcare and its applications," *Comput. Networks*, vol. 153, pp. 113–131, Apr. 2019.

[12] R. Maskeliūnas, R. Damaševičius, and S. Segal, "A Review of Internet of Things Technologies for Ambient Assisted Living Environments," *Futur. Internet*, vol. 11, no. 12, p. 259, Dec. 2019.

[13] J. Cahill, R. Portales, S. McLoughin, N. Nagan, B. Henrichs, and S. Wetherall, "IoT/Sensor-Based Infrastructures Promoting a Sense of Home, Independent Living, Comfort and Wellness," *Sensors*, vol. 19, no. 3, p. 485, Jan. 2019.

[14] Y. Yang, H. Wang, R. Jiang, X. Guo, J. Cheng and Y. Chen, "A Review of IoT-enabled Mobile Healthcare: Technologies, Challenges, and Future Trends," *IEEE Internet Things J.*, doi: 10.1109/JIOT.2022.3144400.

[15] H. Abdelghaffar and M. Abousteit, "Internet of Things (IoT) Interoperability Success Criteria," *Int. J. Enterp. Inf. Syst.*, vol. 17, no. 1, pp. 85–105, Jan. 2021.

[16] Z. N. Aghdam, A. M. Rahmani, and M. Hosseinzadeh, "The Role of the Internet of Things in Healthcare: Future Trends and Challenges," *Comput. Methods Programs Biomed.*, vol. 199, p. 105903, Feb. 2021.

[17] M. N. Bhuiyan, M. M. Rahman, M. M. Billah, and D. Saha, "Internet of Things (IoT): A Review of Its Enabling Technologies in Healthcare Applications, Standards Protocols, Security, and Market Opportunities," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10474–10498, Jul. 2021.

[18] M. Rath and B. Pattanayak, "Technological improvement in modern health care applications using Internet of Things (IoT) and proposal of novel health care approach," *Int. J. Hum. Rights Healthc.*, vol. 12, no. 2, pp. 148–162, May 2019.

[19] B. Pradhan, S. Bhattacharyya, and K. Pal, "IoT-Based Applications in Healthcare Devices," *J. Healthc. Eng.*, vol. 2021, pp. 1–18, Mar. 2021.

[20] J. W. Jolles, "Broad-scale applications of the Raspberry Pi: A review and guide for biologists," *Methods Ecol. Evol.*, vol. 12, no. 9, pp. 1562–1579, Sep. 2021.

[21] A. Polianytsia, O. Starkova, and K. Herasymenko, "Survey of hardware IoT platforms," in *2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*, 2016, pp. 152–153.

[22] V. Vujovic and M. Maksimovic, "Raspberry Pi as a Wireless Sensor node: Performances and constraints," in *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2014, pp. 1013–1018.

[23] H. K. Kondaveeti, N. K. Kumaravelu, S. D. Vanambathina, S. E. Mathe, and S. Vappangi, "A systematic literature review on prototyping with Arduino: Applications, challenges, advantages, and limitations," *Comput. Sci. Rev.*, vol. 40, p. 100364, May 2021.

[24] D. K. Halim, T. C. Ming, N. M. Song, and D. Hartono, "Arduino-based IDE for Embedded Multi-processor System-on-Chip," in *2019 5th International Conference on New Media Studies (CONMEDIA)*, 2019, pp. 135–138.

[25] S.-M. Kim, Y. Choi, and J. Suh, "Applications of the Open-Source Hardware Arduino Platform in the Mining Industry: A Review," *Appl. Sci.*, vol. 10, no. 14, p. 5018, Jul. 2020.

[26] J. Mesquita, D. Guimaraes, C. Pereira, F. Santos, and L. Almeida, "Assessing the ESP8266 WiFi module for the Internet of Things," in *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2018, pp. 784–791.

[27] I. Gunawan, A. Sudianto, and M. Sadali, "Measuring Body Temperature Based Internet of Things (IoT) Using Esp8266 and Firebase," *SISFOTENIKA*, vol. 11, no. 1, p. 91, Jan. 2021.

[28] T. Z. Asici, B. Karaduman, R. Eslampanah, M. Challenger, J. Denil, and H. Vangheluwe, "Applying Model Driven Engineering Techniques to the Development of Contiki-Based IoT Systems," in *2019 IEEE/ACM 1st International Workshop on Software Engineering Research & Practices for the Internet of Things (SERP4IoT)*, 2019, pp. 25–32.

[29] Y. Bin Zikria, M. K. Afzal, F. Ishmanov, S. W. Kim, and H. Yu, "A survey on routing protocols supported by the Contiki Internet of things operating system," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 200–219,

- May 2018.
- [30] C. Sabri, L. Kriaa, and S. L. Azzouz, "Comparison of IoT Constrained Devices Operating Systems: A Survey," in *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, 2017, pp. 369–375.
- [31] F. Jaskani, S. Manzoor, M. Amin, M. Asif, and M. Irfan, "An Investigation on Several Operating Systems for Internet of Things," *EAI Endorsed Trans. Creat. Technol.*, vol. 6, no. 18, p. 160386, Jan. 2019.
- [32] E. Baccelli *et al.*, "RIOT: An Open Source Operating System for Low-End Embedded Devices in the IoT," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4428–4440, Dec. 2018.
- [33] B. Karaduman, M. Challenger, R. Eslampanah, J. Denil, and H. Vangheluwe, "Platform-specific Modeling for RIOT based IoT Systems," in *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*, 2020, pp. 639–646.
- [34] C. Hannon, J. Yan, Y.-A. Liu, and D. Jin, "A Distributed Virtual Time System on Embedded Linux for Evaluating Cyber-Physical Systems," in *Proceedings of the 2019 ACM SIGSIM Conference on Principles of Advanced Discrete Simulation*, 2019, pp. 37–48.
- [35] H. Ben Mansour, L. Chaarabi, and K. Jelassi, "Embedded Linux Hardware/Software Architecture for Electrical Measurement Acquisition," in *Smart Innovation, Systems and Technologies*, 2020, pp. 167–176.
- [36] C. Bell, *Windows 10 for the Internet of Things*. Berkeley, CA: Apress, 2021.
- [37] Z. Syahputa, M. Zarlis, and B. B. Nasution, "Testing Real-Time Applications on Windows 10 IOT Using the Nyquist Theory," *J. Phys. Conf. Ser.*, vol. 1255, p. 012066, Aug. 2019.
- [38] M. Lyaskov, G. Spasov, and G. Petrova, "A practical implementation of smart home energy data storage and control application based on cloud services," in *2017 XXVI International Scientific Conference Electronics (ET)*, 2017, pp. 1–4.
- [39] M. U. H. Al Rasyid, M. H. Mubarrak, and J. A. Nur Hasim, "Implementation of environmental monitoring based on KAA IoT platform," *Bull. Electr. Eng. Informatics*, vol. 9, no. 6, pp. 2578–2587, Dec. 2020.
- [40] A. Kumar and A. Kumar, "6 IoT-based platform for smart farming – Kaa," in *Internet of Things and Machine Learning in Agriculture*, De Gruyter, 2021, pp. 109–130.
- [41] L. O. Aghenta and M. Tariq Iqbal, "Design and implementation of a low-cost, open source IoT-based SCADA system using ESP32 with OLED, ThingsBoard and MQTT protocol," *AIMS Electron. Electr. Eng.*, vol. 4, no. 1, pp. 57–86, 2020.
- [42] M. Henschke, X. Wei, and X. Zhang, "Data Visualization for Wireless Sensor Networks Using ThingsBoard," in *2020 29th Wireless and Optical Communications Conference (WOCC)*, 2020, pp. 1–6.
- [43] W. Tärneberg, V. Chandrasekaran, and M. Humphrey, "Experiences creating a framework for smart traffic control using AWS IOT," in *Proceedings of the 9th International Conference on Utility and Cloud Computing*, 2016, pp. 63–69.
- [44] L. Calderoni, "Preserving context security in AWS IoT Core," in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 2019, pp. 1–5.
- [45] P. Pierleoni, R. Concetti, A. Belli, and L. Palma, "Amazon, Google and Microsoft Solutions for IoT: Architectures and a Performance Comparison," *IEEE Access*, vol. 8, pp. 5455–5470, 2020.
- [46] B. Grados and H. Bedon, "Software Components of an IoT Monitoring Platform in Google Cloud Platform: A Descriptive Research and an Architectural Proposal," in *Communications in Computer and Information Science*, 2020, pp. 153–167.
- [47] N. Mishra and S. Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," *IEEE Access*, vol. 9, pp. 59353–59377, 2021.
- [48] A. Alreshidi and A. Ahmad, "Architecting Software for the Internet of Thing Based Systems," *Futur. Internet*, vol. 11, no. 7, p. 153, Jul. 2019.
- [49] F. Alshohoumi, M. Sarab, A. AlHamadani, and D. Al-Abri, "Systematic Review of Existing IoT Architectures Security and Privacy Issues and Concerns," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 7, 2019.
- [50] W. Kassab and K. A. Darabkh, "A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations," *J. Netw. Comput. Appl.*, vol. 163, p. 102663, Aug. 2020.
- [51] I. Zhou *et al.*, "Internet of Things 2.0: Concepts, Applications, and Future Directions," *IEEE Access*, vol. 9, pp. 70961–71012, 2021.
- [52] K. Liu, Y. Bi, and D. Liu, "Internet of Things based acquisition system of industrial intelligent bar code for smart city applications," *Comput. Commun.*, vol. 150, pp. 325–333, Jan. 2020.
- [53] R. Liu, J. Shen, F. Jiao, and M. Ding, "Deployment Optimization of Perception Layer Nodes in the Internet of Things Based on NB-IoT Technology," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 2021, pp. 202–210.
- [54] P. P. Ray, "A survey on Internet of Things architectures," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 30, no. 3, pp. 291–319, Jul. 2018.
- [55] P. Upadhyay and P. D. Upadhyay, "Internet of things - A Survey," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, pp. 417–438, May 2021.
- [56] J. Dizdarevic, F. Carpio, A. Jukan, and X. Masip-Bruin, "Survey of Communication Protocols for Internet-of-Things and Related Challenges of Fog and Cloud Computing Integration," *ACM Comput. Surv.*, Apr. 2018.
- [57] L. M. Abdulrahman *et al.*, "A State of Art for Smart Gateways Issues and Modification," *Asian J. Res. Comput. Sci.*, pp. 1–13, Apr. 2021.
- [58] A. Kumar, M. Zhao, K.-J. Wong, Y. L. Guan, and P. H. J. Chong, "A Comprehensive Study of IoT and WSN MAC Protocols: Research Issues, Challenges and Opportunities," *IEEE Access*, vol. 6, pp. 76228–76262, 2018.
- [59] J. Zhang, Y. Ye, C. Hu, and B. Li, "Architecture design and demand analysis on application layer of standard system for ubiquitous power Internet of Things," *Glob. Energy Interconnect.*, vol. 4, no. 3, pp. 304–314, Jun. 2021.
- [60] X. Li, Y. Lu, X. Fu, and Y. Qi, "Building the Internet of Things platform for smart maternal healthcare services with wearable devices and cloud computing," *Futur. Gener. Comput. Syst.*, vol. 118, pp. 282–296, May 2021.
- [61] Y. Qian, D. Wu, W. Bao, and P. Lorenz, "The Internet of Things for Smart Cities: Technologies and Applications," *IEEE Netw.*, vol. 33, no. 2, pp. 4–5, Mar. 2019.
- [62] F. Zantalis, G. Koulouras, S. Karabetos, and D. Kandris, "A Review of Machine Learning and IoT in Smart Transportation," *Futur. Internet*, vol. 11, no. 4, p. 94, Apr. 2019.
- [63] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, and E.-H. M. Aggoune, "Internet-of-Things (IoT)-Based Smart Agriculture: Toward Making the Fields Talk," *IEEE Access*, vol. 7, pp. 129551–129583, 2019.
- [64] S. Li, L. Da Xu, and S. Zhao, "5G Internet of Things: A survey," *J. Ind. Inf. Integr.*, vol. 10, pp. 1–9, Jun. 2018.
- [65] M. Lombardi, F. Pascale, and D. Santaniello, "Internet of Things: A General Overview between Architectures, Protocols and Applications," *Information*, vol. 12, no. 2, p. 87, Feb. 2021.
- [66] S. Misra, C. Roy, and A. Mukherjee, "Overview of Internet of Things," in *Introduction to Industrial Internet of Things and Industry 4.0*, CRC Press, 2021, pp. 3–24.
- [67] F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019.
- [68] J.-H. Park, "An Intelligent Service Middleware Based on Sensors in IoT Environments," *Int. J. Softw. Eng. Knowl. Eng.*, vol. 30, no. 04, pp. 523–536, Apr. 2020.
- [69] B. B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols," *Concurr. Comput. Pract. Exp.*, vol. 32, no. 21, Nov. 2020.
- [70] J. Zhang, M. Ma, P. Wang, and X. Sun, "Middleware for the Internet of Things: A survey on requirements, enabling technologies, and solutions," *J. Syst. Archit.*, vol. 117, p. 102098, Aug. 2021.
- [71] M. Palmaccio, G. Dicuozzo, and Z. S. Belyaeva, "The internet of things and corporate business models: A systematic literature review," *J. Bus. Res.*, vol. 131, pp. 610–618, Jul. 2021.
- [72] A. Bujari, M. Furini, F. Mandreoli, R. Martoglia, M. Montangero, and D. Ronzani, "Standards, Security and Business Models: Key Challenges for the IoT Scenario," *Mob. Networks Appl.*, vol. 23, no. 1, pp. 147–154, Feb. 2018.
- [73] J. Silva, J. Rodrigues, J. Al-Muhtadi, R. Rabêlo, and V. Furtado, "Management Platforms and Protocols for Internet of Things: A Survey," *Sensors*, vol. 19, no. 3, p. 676, Feb. 2019.
- [74] G. A. Papakostas and V. Kanakaris, "Internet of things protocols - a survey," *Int. J. Humanit. Technol.*, vol. 1, no. 2, p. 101, 2020.
- [75] M. A. Tariq, M. Khan, M. T. Raza Khan, and D. Kim, "Enhancements

- and Challenges in CoAP—A Survey,” *Sensors*, vol. 20, no. 21, p. 6391, Nov. 2020.
- [76] N. Nikolov, “Research of MQTT, CoAP, HTTP and XMPP IoT Communication protocols for Embedded Systems,” in *2020 XXIX International Scientific Conference Electronics (ET)*, 2020, pp. 1–4.
- [77] G. A. Akpakwu, G. P. Hancke, and A. M. Abu-Mahfouz, “CACC: Context-aware congestion control approach for lightweight CoAP/UDP-based Internet of Things traffic,” *Trans. Emerg. Telecommun. Technol.*, vol. 31, no. 2, Feb. 2020.
- [78] S. Bansal and D. Kumar, “Distance-based congestion control mechanism for CoAP in IoT,” *IET Commun.*, vol. 14, no. 19, pp. 3512–3520, Dec. 2020.
- [79] S.-P. Hsu, Y.-M. Chang, S.-R. Yang, and P.-H. Hsieh, “The Design and Implementation of a Lightweight CoAP-based IoT Framework with Smart Contract Security Guarantee,” in *2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, 2020, pp. 1–6.
- [80] S. Quincozes, T. Emilio, and J. Kazienko, “MQTT Protocol: Fundamentals, Tools and Future Directions,” *IEEE Lat. Am. Trans.*, vol. 17, no. 09, pp. 1439–1448, Sep. 2019.
- [81] B. Mishra and A. Kertesz, “The Use of MQTT in M2M and IoT Systems: A Survey,” *IEEE Access*, vol. 8, pp. 201071–201086, 2020.
- [82] V. M. and S. Sankaranarayanan, “Publish/subscribe based multi-tier edge computational model in Internet of Things for latency reduction,” *J. Parallel Distrib. Comput.*, vol. 127, pp. 18–27, May 2019.
- [83] D. Dinculeană and X. Cheng, “Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices,” *Appl. Sci.*, vol. 9, no. 5, p. 848, Feb. 2019.
- [84] E. Al-Masri *et al.*, “Investigating Messaging Protocols for the Internet of Things (IoT),” *IEEE Access*, vol. 8, pp. 94880–94911, 2020.
- [85] M. Faiqurahman, M. M. Madani, and D. R. Akbi, “Performance of XMPP-Based Gateway for IoT Device Communication Services,” *J. Teknol. dan Sist. Komput.*, vol. 7, no. 4, pp. 127–133, Oct. 2019.
- [86] C.-S. Cho, W.-G. Chen, C.-K. C. Liao, J.-L. Liao, F.-F. Chen, and T.-C. Shen, “Building on the Distributed Energy Resources IoT based IEC 61850 XMPP for TPC,” in *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*, 2019, pp. 61–66.
- [87] C. A. Garcia, J. E. Naranjo, and M. V. Garcia, “Analysis of AMQP for Industrial Internet of Things Based on Low-Cost Automation,” in *Smart Innovation, Systems and Technologies*, 2021, pp. 235–244.
- [88] P. Bhimani and G. Panchal, “Message Delivery Guarantee and Status Update of Clients Based on IoT-AMQP,” in *Lecture Notes in Networks and Systems*, 2018, pp. 15–22.
- [89] G. P. Naik and A. U. Bapat, “A Brief Comparative Analysis on Application Layer Protocols of Internet of Things: MQTT, CoAP, AMQP and HTTP,” *Int. J. Comput. Sci. Mob. Comput.*, vol. 9, no. 9, pp. 135–141, Sep. 2020.
- [90] F. Karatas and I. Korpeoglu, “Fog-Based Data Distribution Service (F-DAD) for Internet of Things (IoT) applications,” *Futur. Gener. Comput. Syst.*, vol. 93, pp. 156–169, Apr. 2019.
- [91] T. Alam, B. Rababah, A. Ali, and S. Qamar, “Distributed Intelligence at the Edge on IoT Networks,” *Ann. Emerg. Technol. Comput.*, vol. 4, no. 5, pp. 1–18, Dec. 2020.
- [92] R. S. Auliva, R.-K. Sheu, D. Liang, and W.-J. Wang, “IIoT Testbed: A DDS-Based Emulation Tool for Industrial IoT Applications,” in *2018 International Conference on System Science and Engineering (ICSSE)*, 2018, pp. 1–4.
- [93] C. Gündoğan, P. Kietzmann, T. C. Schmidt, and M. Wählich, “Designing a LoWPAN convergence layer for the Information Centric Internet of Things,” *Comput. Commun.*, vol. 164, pp. 114–123, Dec. 2020.
- [94] M. K. Shah and L. K. Sharma, “Study on 6LoWPAN Routing Protocols with SD aspects in IoT,” in *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)/I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2018 2nd International Conference on, 2018, pp. 60–65.
- [95] S. Zeadally, F. Siddiqui, and Z. Baig, “25 Years of Bluetooth Technology,” *Futur. Internet*, vol. 11, no. 9, p. 194, Sep. 2019.
- [96] E. Garcia-Espinosa, O. Longoria-Gandara, I. Pegueros-Lepe, and A. Veloz-Guerrero, “Power Consumption Analysis of Bluetooth Low Energy Commercial Products and Their Implications for IoT Applications,” *Electronics*, vol. 7, no. 12, p. 386, Dec. 2018.
- [97] K. E. Jeon, J. She, P. Soonsawad, and P. C. Ng, “BLE Beacons for Internet of Things Applications: Survey, Challenges, and Opportunities,” *IEEE Internet Things J.*, vol. 5, no. 2, pp. 811–828, Apr. 2018.
- [98] Y. R. Hamdy and A. I. Alghannam, “Evaluation of ZigBee Topology Effect on Throughput and End to End Delay Due to Different Transmission Bands for IoT Applications,” *J. Commun. Softw. Syst.*, vol. 16, no. 3, pp. 254–259, Sep. 2020.
- [99] H. Zemrane, Y. Baddi, and A. Hasbi, “Internet of Things Industry 4.0 Ecosystem Based on Zigbee Protocol,” in *Advances in Intelligent Systems and Computing*, 2021, pp. 249–260.
- [100] M. Gupta and S. Singh, “A Survey on the ZigBee Protocol, It’s Security in Internet of Things (IoT) and Comparison of ZigBee with Bluetooth and Wi-Fi,” 2021, pp. 473–482.
- [101] M. Haghi Kashani, M. Madanipour, M. Nikravan, P. Asghari, and E. Mahdipour, “A systematic review of IoT in healthcare: Applications, techniques, and trends,” *J. Netw. Comput. Appl.*, vol. 192, p. 103164, Oct. 2021.
- [102] G. Muhammad, F. Alshehri, F. Karray, A. E. Saddik, M. Alsulaiman, and T. H. Falk, “A comprehensive survey on multimodal medical signals fusion for smart healthcare systems,” *Inf. Fusion*, vol. 76, pp. 355–375, Dec. 2021.
- [103] S. Selvaraj and S. Sundaravaradhan, “Challenges and opportunities in IoT healthcare systems: a systematic review,” *SN Appl. Sci.*, vol. 2, no. 1, p. 139, Jan. 2020.
- [104] Y. A. Qadri, A. Nauman, Y. Bin Zikria, A. V. Vasilakos, and S. W. Kim, “The Future of Healthcare Internet of Things: A Survey of Emerging Technologies,” *IEEE Commun. Surv. Tutorials*, vol. 22, no. 2, pp. 1121–1167, 2020.
- [105] V. S. Naresh, S. S. Pericherla, P. Sita Rama Murty, and S. Reddi, “Internet of Things in Healthcare: Architecture, Applications, Challenges, and Solutions,” *Comput. Syst. Sci. Eng.*, vol. 35, no. 6, pp. 411–421, 2020.
- [106] A. Rahaman, M. Islam, M. Islam, M. Sadi, and S. Nooruddin, “Developing IoT Based Smart Health Monitoring Systems: A Review,” *Rev. d’Intelligence Artif.*, vol. 33, no. 6, pp. 435–440, Dec. 2019.
- [107] G. Marques, J. Saini, I. M. Pires, N. Miranda, and R. Pitarma, “Internet of Things for Enhanced Living Environments, Health and Well-Being: Technologies, Architectures and Systems,” in *Advances in Intelligent Systems and Computing*, 2020, pp. 616–631.
- [108] N. Y. Philip, J. J. P. C. Rodrigues, H. Wang, S. J. Fong, and J. Chen, “Internet of Things for In-Home Health Monitoring Systems: Current Advances, Challenges and Future Directions,” *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 300–310, Feb. 2021.
- [109] H. Ahmadi, G. Arji, L. Shahmoradi, R. Safdari, M. Nilashi, and M. Alizadeh, “The application of internet of things in healthcare: a systematic literature review and classification,” *Universal Access in the Information Society*, 2019.
- [110] M. H. Islam, A. Rahaman, and M. R. Islam, “Development of Smart Healthcare Monitoring System in IoT Environment,” *SN Comput. Sci.*, vol. 1, no. 3, p. 185, May 2020.
- [111] M. A. Serhani, H. T. El Kassabi, H. Ismail, and A. Nujum Navaz, “ECG Monitoring Systems: Review, Architecture, Processes, and Key Challenges,” *Sensors*, vol. 20, no. 6, p. 1796, Mar. 2020.
- [112] P. K. Vishwakarma and R. Singh, “A – Review on IoT-Assisted ECG Monitoring Framework for Health Care Applications,” in *2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT)*, 2021, pp. 203–207.
- [113] T. Wu, J.-M. Redouté, and M. Yuce, “A Wearable, Low-Power, Real-Time ECG Monitor for Smart T-shirt and IoT Healthcare Applications,” in *Internet of Things*, 2019, pp. 165–173.
- [114] T. Shaown, I. Hasan, M. M. R. Mim, and M. S. Hossain, “IoT-based Portable ECG Monitoring System for Smart Healthcare,” in *2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT)*, 2019, pp. 1–5.
- [115] H. Djelouat *et al.*, “Real-time ECG monitoring using compressive sensing on a heterogeneous multicore edge-device,” *Microprocess. Microsyst.*, vol. 72, p. 102839, Feb. 2020.
- [116] M. L. Sahu, M. Atulkar, M. K. Ahirwal, and A. Ahamad, “IoT-enabled cloud-based real-time remote ECG monitoring system,” *J. Med. Eng. Technol.*, vol. 45, no. 6, pp. 473–485, Aug. 2021.
- [117] S. Basu, A. Sengupta, A. Das, M. Ghosh, and S. Barman (Mandal), “IoT-Based Real-Time Remote ECG Monitoring System,” in *Lecture Notes in Networks and Systems*, 2021, pp. 23–28.
- [118] F. Lamonaca *et al.*, “An Overview on Internet of Medical Things in Blood Pressure Monitoring,” in *2019 IEEE International Symposium on Medical Measurements and Applications (MeMeA)*, 2019, pp. 1–6.
- [119] L. R. Krakoff, “Home Blood Pressure Monitoring,” *Hypertension*, vol.

- 63, no. 4, pp. 670–671, Apr. 2014.
- [120] Q. Xin and J. Wu, “A novel wearable device for continuous, non-invasive blood pressure measurement,” *Comput. Biol. Chem.*, vol. 69, pp. 134–137, Aug. 2017.
- [121] B. Singh, S. Urooj, S. Mishra, and S. Haldar, “Blood Pressure Monitoring System using Wireless technologies,” *Procedia Comput. Sci.*, vol. 152, pp. 267–273, 2019.
- [122] N. Hashim, N. Norddin, F. Idris, S. N. I. Mohd Yusoff, and M. Zahari, “IoT blood pressure monitoring system,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 19, no. 3, p. 1384, Sep. 2020.
- [123] A. EL ATTAOUL, S. Largo, A. Jilbab, and A. Bourouhou, “Wireless medical sensor network for blood pressure monitoring based on machine learning for real-time data classification,” *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 9, pp. 8777–8792, Sep. 2021.
- [124] P. D. P. Adi and A. Kitagawa, “ZigBee Radio Frequency (RF) Performance on Raspberry Pi 3 for Internet of Things (IoT) based Blood Pressure Sensors Monitoring,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 5, 2019.
- [125] T. Mohanraj, B. Arunkumar, S. ShahulHammed, and R. Santhosh, “A Review on Internet of Things (IoT) Based Pulse Rate, Blood Pressure, Body Temperature Monitoring System,” in *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2020, pp. 78–79.
- [126] H. Ota *et al.*, “3D Printed ‘Earable’ Smart Devices for Real-Time Detection of Core Body Temperature,” *ACS Sensors*, vol. 2, no. 7, pp. 990–997, Jul. 2017.
- [127] N. A. Zakaria, F. N. B. Mohd Saleh, and M. A. A. Razak, “IoT (Internet of Things) Based Infant Body Temperature Monitoring,” in *2018 2nd International Conference on BioSignal Analysis, Processing and Systems (ICBAPS)*, 2018, pp. 148–153.
- [128] A. A. Rahimoon, M. N. Abdullah, and I. Taib, “Design of a contactless body temperature measurement system using Arduino,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 19, no. 3, p. 1251, Sep. 2020.
- [129] W. Boonsong, N. Senajit, and P. Prasongchan, “Contactless Body Temperature Monitoring of In-Patient Department (IPD) Using 2.4 GHz Microwave Frequency via the Internet of Things (IoT) Network,” *Wirel. Pers. Commun.*, Nov. 2021.
- [130] B. Fang, F. Sun, Z. Quan, H. Liu, and J. Shan, “Smart Bracelet System for Temperature Monitoring and Movement Tracking Analysis,” *J. Healthc. Eng.*, vol. 2021, pp. 1–11, Jul. 2021.
- [131] T. M. Fernández-Caramés, I. Froiz-Míguez, O. Blanco-Novoa, and P. Fraga-Lamas, “Enabling the Internet of Mobile Crowdsourcing Health Things: A Mobile Fog Computing, Blockchain and IoT Based Continuous Glucose Monitoring System for Diabetes Mellitus Research and Care,” *Sensors*, vol. 19, no. 15, p. 3319, Jul. 2019.
- [132] K. Dziergowska, M. B. Łabowska, M. Gąsior-Głogowska, B. Kmiecik, and J. Detyna, “Modern noninvasive methods for monitoring glucose levels in patients: a review,” *Bio-Algorithms and Med-Systems*, vol. 15, no. 4, Dec. 2019.
- [133] A. Alarcón-Paredes, V. Francisco-García, I. P. Guzmán-Guzmán, J. Cantillo-Negrete, R. E. Cuevas-Valencia, and G. A. Alonso-Silverio, “An IoT-Based Non-Invasive Glucose Level Monitoring System Using Raspberry Pi,” *Appl. Sci.*, vol. 9, no. 15, p. 3046, Jul. 2019.
- [134] T. N. Gia *et al.*, “IoT-based continuous glucose monitoring system: A feasibility study,” *Procedia Comput. Sci.*, vol. 109, pp. 327–334, 2017.
- [135] C. F. Aizat Rahmat, M. A. Su, E. L.M. Mohd Addi, M. Yeong, “GluQo: IoT-Based Non-invasive Blood Glucose Monitoring,” *J. Telecommun. Electron. Comput. Eng.*, vol. 9, no. 3–9, pp. 71–75, 2017.
- [136] F. Valenzuela, A. García, E. Ruiz., M. Vázquez, J. Cortez, and A. Espinoza, “An IoT-Based Glucose Monitoring Algorithm to Prevent Diabetes Complications,” *Appl. Sci.*, vol. 10, no. 3, p. 921, Jan. 2020.
- [137] R. Bin Anis, Siti Nur Shahidah binti Alias, “A Portable Non-Invasive Blood Glucose Monitoring Device with IoT,” *Evol. Electr. Electron. Eng.*, vol. 2, no. 1, pp. 36–44, 2021.
- [138] W. Zhong, Z. Ji, and C. Sun, “A Review of Monitoring Methods for Cerebral Blood Oxygen Saturation,” *Healthcare*, vol. 9, no. 9, p. 1104, Aug. 2021.
- [139] S. Basu, S. Saha, S. Pandit, and S. Barman, “Smart Health Monitoring System for Temperature, Blood Oxygen Saturation, and Heart Rate Sensing with Embedded Processing and Transmission Using IoT Platform,” in *Advances in Intelligent Systems and Computing*, 2020, pp. 81–91.
- [140] L. Phuoc Son, N. Thi Anh Thu, and N. Trung Kien, “Design an IoT wrist-device for SpO2 measurement,” in *2017 International Conference on Advanced Technologies for Communications (ATC)*, 2017, pp. 144–149.
- [141] Q. Chen and L. Tang, “A wearable blood oxygen saturation monitoring system based on bluetooth low energy technology,” *Comput. Commun.*, vol. 160, pp. 101–110, Jul. 2020.
- [142] Q. Zhang, D. Arney, J. M. Goldman, E. M. Isselbacher, and A. A. Armoundas, “Design Implementation and Evaluation of a Mobile Continuous Blood Oxygen Saturation Monitoring System,” *Sensors*, vol. 20, no. 22, p. 6581, Nov. 2020.
- [143] R. R. Adiputra, S. Hadiyoso, and Y. S. Hariyani, “Internet of Things: Low Cost and Wearable SpO2 Device for Health Monitoring,” *Int. J. Electr. Comput. Eng.*, vol. 8, no. 2, p. 939, Apr. 2018.
- [144] B. Utomo, Triwiyanto, S. Luthfiah, U. Mudjiono, and T. Hamzah, “The Real-Time Vital Sign Monitor for Heart Rate and SPO 2 Parameter Using Internet of Things Technology,” *J. Phys. Conf. Ser.*, vol. 1373, no. 1, p. 012028, Nov. 2019.
- [145] A. A. Qaffas, R. Hoque, and N. Almazmomi, “The Internet of Things and Big Data Analytics for Chronic Disease Monitoring in Saudi Arabia,” *Telemed. e-Health*, vol. 27, no. 1, pp. 74–81, Jan. 2021.
- [146] T. Amira, I. Dan, B. Az-eddine, H. H. Ngo, G. Said, and W.-W. Katarzyna, “Monitoring chronic disease at home using connected devices,” in *2018 13th Annual Conference on System of Systems Engineering (SoSE)*, 2018, pp. 400–407.
- [147] A. N. Shihab, M. J. Mokarrama, R. Karim, S. Khatun, and M. S. Arefin, “An IoT-Based Heart Disease Detection System Using RNN,” in *Advances in Intelligent Systems and Computing*, 2021, pp. 535–545.
- [148] M. K. Gawali and C. Rambabu, “IoT Model for Heart Disease Detection Using Machine Learning (ML) Techniques,” in *Techno-Societal 2020*, 2021.
- [149] A. Hebbale, G. Vinay, B. V. Krishna, and J. Shah, “IoT and Machine Learning based Self Care System for Diabetes Monitoring and Prediction,” in *2021 2nd Global Conference for Advancement in Technology (GCAT)*, 2021, pp. 1–7.
- [150] P. R. Anisha and C. K. K. Reddy, “Early Detection of Diabetes Using Machine Learning Algorithms and Internet of Things: ADPA,” in *Lecture Notes in Networks and Systems*, 2021, pp. 79–85.
- [151] S. T. U. Shah, F. Badshah, F. Dad, N. Amin, and M. A. Jan, “Cloud-Assisted IoT-Based Smart Respiratory Monitoring System for Asthma Patients,” in *EAI/Springer Innovations in Communication and Computing*, 2019, pp. 77–86.
- [152] A. K. Prasad, “SMART Asthma Alert Using IoT and Predicting Threshold Values Using Decision Tree Classifier,” in *Lecture Notes in Networks and Systems*, 2021, pp. 141–150.
- [153] O. Rehman, Z. Farrukh, A. Al-Busaidi, K. Cha, S. Park, and I. Rahman, “IoT Powered Cancer Observation System,” in *The 9th International Conference on Smart Media and Applications*, 2020, pp. 313–318.
- [154] A. Onasanya and M. Elshakankiri, “Smart integrated IoT healthcare system for cancer care,” *Wirel. Networks*, vol. 27, no. 6, pp. 4297–4312, Aug. 2021.
- [155] J. Huang, X. Wu, W. Huang, X. Wu, and S. Wang, “Internet of things in health management systems: A review,” *Int. J. Commun. Syst.*, vol. 34, no. 4, Mar. 2021.
- [156] K. H. So, C. W. Ting, C. P. Lee, T. T.-N. Lam, S. C. Chiang, and Y. T. Cheung, “Medication Management Service for Old Age Homes in Hong Kong Using Information Technology, Automation Technology, and the Internet of Things: Pre-Post Interventional Study,” *JMIR Med. Informatics*, vol. 9, no. 2, p. e24280, Feb. 2021.
- [157] S. A. Bharadwaj, D. Yarravarapu, S. C. K. Reddy, T. Prudhvi, K. S. P. Sandeep, and O. S. D. Reddy, “Enhancing healthcare using m-Care box (Monitoring non-compliance of medication),” in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2017, pp. 352–356.
- [158] M. Srinivas, P. Durgaprasadarao, and V. N. P. Raj, “Intelligent medicine box for medication management using IoT,” in *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, 2018, pp. 32–34.
- [159] G. Latif, A. Shankar, J. M. Alghazo, V. Kalyanasundaram, C. S. Boopathi, and M. Arfan Jaffar, “I-CARES: advancing health diagnosis and medication through IoT,” *Wirel. Networks*, vol. 26, no. 4, pp. 2375–2389, May 2020.
- [160] H.-L. Tsai, C. H. Tseng, L.-C. Wang, and F.-S. Juang, “Bidirectional smart pill box monitored through internet and receiving reminding message from remote relatives,” in *2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW)*, 2017, pp. 393–394.
- [161] B. Ayshwarya and R. Velmurugan, “Intelligent and Safe Medication

- Box In Health IoT Platform for Medication Monitoring System with Timely Reminders,” in *2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2021, pp. 1828–1831.
- [162] P. A. Harsha Vardhini, M. S. Harsha, P. N. Sai, and P. Srikanth, “IoT based Smart Medicine Assistive System for Memory Impairment Patient,” in *2020 12th International Conference on Computational Intelligence and Communication Networks (CICN)*, 2020, pp. 182–186.
- [163] S. M. A. Ullah, M. M. Islam, S. Mahmud, S. Nooruddin, S. M. T. U. Raju, and M. R. Haque, “Scalable Telehealth Services to Combat Novel Coronavirus (COVID-19) Pandemic,” *SN Comput. Sci.*, vol. 2, no. 1, p. 18, Feb. 2021.
- [164] C. M. Graham and N. Jones, “Impact of IoT on geriatric telehealth,” *Work. with Older People*, vol. 24, no. 3, pp. 231–243, Aug. 2020.
- [165] Md. Rokonzaman, M. I. Hossain, T. Islam, P. P. Sarkar, M. R. Islam, and N. Amin, “Design and Implementation of Telehealth Device: Linking IoT Sensors to Cloud Networks,” in *2020 IEEE-EMBS Conference on Biomedical Engineering and Sciences (IECBES)*, 2021, pp. 281–285.
- [166] D. Ganesh, G. Seshadri, S. Sokkanarayanan, P. Bose, S. Rajan, and M. Sathiyarayanan, “AutoImpilo: Smart Automated Health Machine using IoT to Improve Telemedicine and Telehealth,” in *Proceedings of the International Conference on Smart Technologies in Computing, Electrical and Electronics, ICSTCEE 2020*, 2020.
- [167] K. M. Tsiouris *et al.*, “Designing interoperable telehealth platforms: bridging IoT devices with cloud infrastructures,” *Enterp. Inf. Syst.*, vol. 14, no. 8, pp. 1194–1218, Sep. 2020.
- [168] T. Hewa, A. Braeken, M. Ylianttila, and M. Liyanage, “Multi-Access Edge Computing and Blockchain-based Secure Telehealth System Connected with 5G and IoT,” in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, 2020, pp. 1–6.
- [169] H. Hamil *et al.*, “Design of a secured telehealth system based on multiple biosignals diagnosis and classification for application,” *Expert Syst.*, Jul. 2021.
- [170] D. Pal, S. Funilkul, N. Charoenkitkarn, and P. Kanthamanon, “Internet-of-Things and Smart Homes for Elderly Healthcare: An End User Perspective,” *IEEE Access*, vol. 6, pp. 10483–10496, 2018.
- [171] J. P. Lousado and S. Antunes, “Monitoring and Support for Elderly People Using LoRa Communication Technologies: IoT Concepts and Applications,” *Futur. Internet*, vol. 12, no. 11, p. 206, Nov. 2020.
- [172] A. Abdelgawad, K. Yelamarthi, and A. Khattab, “IoT-Based Health Monitoring System for Active and Assisted Living,” in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICTE*, 2017, pp. 11–20.
- [173] R. K. Nath and H. Thapliyal, “Wearable Health Monitoring System for Older Adults in a Smart Home Environment,” in *2021 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2021, pp. 390–395.
- [174] O. Debauche, S. Mahmoudi, P. Manneback, and A. Assila, “Fog IoT for Health: A new Architecture for Patients and Elderly Monitoring,” *Procedia Comput. Sci.*, vol. 160, pp. 289–297, 2019.
- [175] J. Boobalan and M. Malleswaran, “A Novel and Customizable Framework for IoT Based Smart Home Nursing for Elderly Care,” in *Lecture Notes on Data Engineering and Communications Technologies*, 2020, pp. 27–38.
- [176] A. Srinivasan *et al.*, “Elder Care System using IoT and Machine Learning in AWS Cloud,” in *2020 IEEE 17th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)*, 2020, pp. 92–98.
- [177] M. Frustaci, P. Pace, G. Aloï, and G. Fortino, “Evaluating critical security issues of the IoT world: Present and future challenges,” *IEEE Internet Things J.*, vol. 5, no. 4, 2018.
- [178] M. Masud *et al.*, “A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care,” *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15694–15703, Nov. 1, 2021.
- [179] M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid and G. Muhammad, “Lightweight and Anonymity-Preserving User Authentication Scheme for IoT-Based Healthcare,” *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2649–2656, Feb. 15, 2022.
- [180] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, “Addressing Security and Privacy Issues of IoT Using Blockchain Technology,” *IEEE Internet Things J.*, vol. 8, no. 2, 2021.
- [181] Y. Zhao, X. Yang, Y. Yu, B. Qin, X. Du and M. Guizani, “Blockchain-Based Auditable Privacy-Preserving Data Classification for Internet of Things,” *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2468–2484, 15 Feb. 15, 2022.
- [182] R. Sanchez-Iborra and A. F. Skarmeta, “TinyML-Enabled Frugal Smart Objects: Challenges and Opportunities,” *IEEE Circuits Syst. Mag.*, vol. 20, no. 3, 2020.
- [183] D. L. Dutta and S. Bharali, “TinyML Meets IoT: A Comprehensive Survey,” *Internet of Things*, vol. 16, 2021.
- [184] V. Gazis, “A Survey of Standards for Machine-to-Machine and the Internet of Things,” *IEEE Communications Surveys and Tutorials*, vol. 19, no. 1, 2017.
- [185] S. Wan, J. Lu, P. Fan, and K. B. Letaief, “Toward Big Data Processing in IoT: Path Planning and Resource Management of UAV Base Stations in Mobile-Edge Computing System,” *IEEE Internet Things J.*, vol. 7, no. 7, 2020.
- [186] M. Syafrudin, G. Alfian, N. L. Fitriyani, and J. Rhee, “Performance analysis of IoT-based sensor, big data processing, and machine learning model for real-time monitoring system in automotive manufacturing,” *Sensors (Switzerland)*, vol. 18, no. 9, 2018.
- [187] D. D. Sánchez-Gallegos *et al.*, “From the edge to the cloud: A continuous delivery and preparation model for processing big IoT data,” *Simul. Model. Pract. Theory*, vol. 105, 2020.
- [188] Y. N. Malek *et al.*, “On the use of IoT and Big Data Technologies for Real-time Monitoring and Data Processing,” in *Procedia Computer Science*, 2017, vol. 113.
- [189] G. Signoretto, M. Silva, P. Andrade, I. Silva, E. Sisinni, and P. Ferrari, “An evolving tinyml compression algorithm for iot environments based on data eccentricity,” *Sensors*, vol. 21, no. 12, 2021.
- [190] K. Nolan and M. Kelly, “IPv6 convergence for IoT cyber-physical systems,” *Inf.*, vol. 9, no. 4, 2018.
- [191] T. Savolainen, J. Soinen, and B. Silverajan, “IPv6 addressing strategies for IoT,” *IEEE Sens. J.*, vol. 13, no. 10, 2013.
- [192] A. E. Khaled, A. Helal, W. Lindquist, and C. Lee, “IoT-DDL-Device Description Language for the ‘T’ in IoT,” *IEEE Access*, vol. 6, 2018.
- [193] M. Zúñiga-Prieto, D. Rodríguez, J. Rodríguez, L. Solano, E. Insfran, and S. Abrahao, “IOT-ADL: An ADL for describing cloud IoT applications,” *J. Comput.*, vol. 29, no. 6, 2018.
- [194] A. S. Pillai, G. S. Chandraprasad, A. S. Khwaja, and A. Anpalagan, “A service oriented IoT architecture for disaster preparedness and forecasting system,” *Internet of Things (Netherlands)*, vol. 14, 2021.
- [195] S. Maurya and K. Mukherjee, “An energy efficient architecture of IoT based on service oriented architecture (SOA),” *Inform.*, vol. 43, no. 1, 2019.
- [196] L. Li, S. Li, and S. Zhao, “QoS-Aware scheduling of services-oriented internet of things,” *IEEE Trans. Ind. Informatics*, vol. 10, no. 2, 2014.
- [197] K. Panagidi, C. Anagnostopoulos, A. Chalvatzaras, and S. Hadjijefthymiades, “To transmit or not to transmit: Controlling communications in the mobile iot domain,” *ACM Trans. Internet Technol.*, vol. 20, no. 3, 2020.
- [198] X. Xiong, K. Zheng, L. Lei, and L. Hou, “Resource allocation based on deep reinforcement learning in IoT edge computing,” *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, 2020.
- [199] X. Wei, J. Zhao, L. Zhou, and Y. Qian, “Broad Reinforcement Learning for Supporting Fast Autonomous IoT,” *IEEE Internet Things J.*, vol. 7, no. 8, 2020.
- [200] S. M. Hatim, S. J. Elias, N. Awang, and M. Y. Darus, “VANETs and Internet of Things (IoT): A discussion,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 12, no. 1, 2018.
- [201] Y. Mo, L. Xing, W. Guo, S. Cai, Z. Zhang, and J. Jiang, “Reliability Analysis of IoT Networks with Community Structures,” *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, 2020.
- [202] K. Azghiou, M. El Mouhib, M. A. Koulali, and A. Benali, “An end-to-end reliability framework of the internet of things,” *Sensors (Switzerland)*, vol. 20, no. 9, 2020.
- [203] L. Xing, “Reliability in Internet of Things: Current Status and Future Perspectives,” *IEEE Internet Things J.*, vol. 7, no. 8, 2020.
- [204] O. Novo, “Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT,” *IEEE Internet Things J.*, vol. 5, no. 2, 2018.
- [205] A. Javed, A. Malhi, T. Kinnunen, and K. Framling, “Scalable IoT Platform for Heterogeneous Devices in Smart Environments,” *IEEE Access*, vol. 8, 2020.
- [206] M. Noura, M. Atiquzzaman, and M. Gaedke, “Interoperability in Internet of Things: Taxonomies and Open Challenges,” *Mob. Networks Appl.*, vol. 24, no. 3, 2019.
- [207] T. R. Gadekallu *et al.*, “Blockchain for Edge of Things: Applications, Opportunities, and Challenges,” *IEEE Internet Things J.*, vol. 9, no. 2, pp. 964–988, 15 Jan. 15, 2022.
- [208] Y. Liu, M. Peng, G. Shou, Y. Chen and S. Chen, “Toward Edge

Intelligence: Multiaccess Edge Computing for 5G and Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6722-6747, Aug. 2020.



**Md. Milon Islam** is currently pursuing his PhD at the Centre for Pattern Analysis and Machine Intelligence in the Department of Electrical and Computer Engineering at the University of Waterloo, Canada. He received his B.Sc. and M.Sc. degree in Computer Science and Engineering (CSE) from the Khulna University of Engineering & Technology, Khulna, Bangladesh, in 2016 and 2019 respectively, where he is currently

working as an Assistant Professor (on leave) in CSE. In 2017, he joined the Department of Computer Science and Engineering, Khulna University of Engineering & Technology, as a Lecturer. He has published several numbers of research papers in peer reviewed journals, book chapters and conferences. In addition, he is reviewer of several reputed journals and conferences. His research interests include machine learning and its application, deep learning, intelligent systems design, health informatics, Internet of Things (IoT), and to solve real life problems with the concept of computer science.



**Sheikh Nooruddin** is currently pursuing his Master of Applied Science (MAsc) degree in Electrical and Computer Engineering (ECE) with a specialization in Pattern Analysis and Machine Intelligence (PAMI) at the University of Waterloo, Ontario, Canada. He received his B.Sc. Eng. in Computer Science and Engineering degree from Khulna University of Engineering & Technology, Bangladesh in 2020.

His research interests include computer vision, artificial intelligence, human activity recognition, Internet of things, and medical signal processing. He has authored and co-authored multiple journals and conference articles published by reputed peer-reviewed international publishers including IEEE, Elsevier, and Springer.



**Fakhri Karray** is a Professor and Provost of the Mohamed Bin Zayed University of AI in the UAE. He has served as the University Research Chair Professor in Electrical and Computer Engineering and the founding co-director of the Institute of Artificial Intelligence at the University of Waterloo. He holds the Loblaw's Research Chair in Artificial Intelligence. Dr. Karray's research work spans the areas of intelligent systems and operational artificial

intelligence as applied to smart devices and man machine interaction systems through speech, gesture, and natural language. He has authored extensively in these areas and has disseminated his work in journals, conference proceedings, and textbooks. He is the co-author of two dozen US patents, has chaired/co-chaired several international conferences in his area of expertise and has served as keynote/plenary speaker on numerous occasions. He has served as the associate editor/guest editor for a variety of leading journals in the field, including the IEEE Transactions on Cybernetics, the IEEE Transactions on Neural Networks and Learning Systems, the IEEE Transactions on Mechatronics, the IEEE Computational Intelligence Magazine. He has served as the University of Waterloo's Academic Advisor for Amazon's Alexa Fund Fellowship Program and is a Fellow of the Canadian Academy of

Engineering, a Fellow of the Engineering Institute of Canada and a Fellow of the IEEE.



**Ghulam Muhammad** (Senior Member, IEEE) is a professor in the Department of Computer Engineering, College of Computer and Information Sciences at King Saud University (KSU), Riyadh, Saudi Arabia. Prof. Ghulam received his Ph.D. degree in Electronic and Information Engineering from Toyohashi University and Technology, Japan in 2006, M.S. degree from the same university in 2003. He received his B.S. degree in Computer Science and Engineering

from Bangladesh University of Engineering and Technology in 1997. He was a recipient of the Japan Society for Promotion and Science (JSPS) fellowship from the Ministry of Education, Culture, Sports, Science and Technology, Japan. His research interests include signal processing, machine learning, IoTs, medical signal and image analysis, AI, and biometrics. Prof. Ghulam has authored and co-authored more than 300 publications including IEEE / ACM / Springer / Elsevier journals, and flagship conference papers. He owns two U.S. patents. He received the best faculty award of Computer Engineering department at KSU during 2014-2015. He has supervised more than 15 Ph.D. and Master Theses.