Marc Jayson Baucas, Petros Spachos, and Stefano Gregori

Internet-of-Things Devices and Assistive Technologies for Health Care

Applications, challenges, and opportunities

©SHUTTERSTOCK.COM/TEX VECTOR

Medical conditions and cases are growing at a rapid pace, and physical space is starting to be constrained. Hospitals and clinics no longer have the ability to accommodate large numbers of incoming patients. It is clear that the health industry needs to improve the current state of its valuable and limited resources. The evolution of Internet-of-Things (IoT) devices along with assistive technologies can alleviate the problem in health care by providing a convenient and easy means of accessing health-care services wirelessly. There is a plethora of IoT devices and potential applications that can take advantage of the unique characteristics that these technologies can offer. However, at the same time, these services pose novel challenges that need to be properly addressed. In this article, we review some popular categories of IoT-based applications for health care along with their devices. We then describe the challenges and discuss how research can properly address the open issues and improve the already-existing implementations in health care. Further possible solutions, including machine learning (ML) techniques, are also discussed to show their potential as viable solutions for future health-care applications.

Introduction

The recent pandemic has revealed underlying limitations, inequities, and gaps in universal health-care access. The COVID-19 disease has exposed the centrality of health, both as an outcome and as an engine for economic and social development. Even advanced health-care systems face unprecedented challenges caused by demographic, epidemiological, and health transitions. The hard-learned lessons for the health sector dictate improvements in both the effectiveness and efficiency of services. Health-care services need to take full advantage of new technologies for upgrading their capacity to prevent, diagnose, and treat diseases. The IoT concept is rapidly spreading in the health-care sector because of its ability to effectively integrate its services [1]. The IoT enables people and objects to be connected anytime and anywhere, via any network and service. IoT networks can operate within health-care centers, they can be scaled up to provide services

Digital Object Identifier 10.1109/MSP.2021.3075929
Date of current version: 28 June 2021

to urban communities, and they can connect patients and health-care providers over longer distances, thereby lowering geographical barriers to health-care access and the burden on health-care facilities.

E-health services relying on electronic devices and smart environments [2] are leading to a proliferation of assistive technologies based on wireless networks and IoT implementations. These technologies equip patients with devices that monitor and aid certain aspects of their health and well-being. The collected data are shared between an IoT device and a central server, usually through a wireless network. A data hierarchy is constructed to allow patients to be remotely screened for any anomalies and aided for certain health conditions.

Although IoT devices along with assistive technologies provide significant benefits to health-care services, they also pose challenges, specifically with regard to patient privacy, data latency, service interactability, device constraints, and scalability. The privacy and security of a patient's personal information have always been a concern in health-care services [3]. IoT-based services make use of wireless communication to transfer data, which has vulnerabilities and may result in user information being compromised [4].

Wireless communications also have limitations in terms of data transmission. While continuous transmission of data could result in exhaustion of the server and congestion of the network [5], a discontinuous dataflow could be detrimental to the service in applications that need the data to reach the server in real time. Regarding interactability, in passive assistive technologies, which only collect or transmit data, the health center is responsible for translating these data into useful information to screen or diagnose the patient. However, the latency caused by data transmission and processing limits the ability to respond to emergencies in real time. Systems that allow real-time interactions between the health center and the patient can lead to better, more responsive, and reliable services.

At the same time, the constraints of the devices used in collecting and transmitting the data limit the effectiveness of the service, particularly with regard to the ability of the devices to keep up with the demands of the service in terms of power consumption and processing requirements over time. Finally, the scalability of the overall service is also important as it defines its capacity in terms of how many users it can handle. An application that cannot scale along with the growth of its devices and users will not be able to keep up with the needs of the communities that use it. As a result, services that suffer from device constraints and scalability issues lose their credibility and viability as products in the health-care industry.

This article reviews the available IoT-based services in health care and discusses some representative IoT-based health-care applications along with their challenges and the ensuing research opportunities. As such, we cover the following main areas:

1) an overview of IoT-based applications in health care, where we present some popular IoT-based applications for health care along with their advantages and three different approaches for their data processing location
2) devices and assistive technologies in IoT-based health care, where we discuss these topics and how they can enhance the current state of the art in health care. We present three main types along with examples
3) the challenges in IoT-based health-care services, where we discuss several important issues
4) research approaches and opportunities, where we focus on existing solutions for the challenges and further discuss potential opportunities for researchers.

Overview of IoT-based applications in health care

Health care is an industry that has adopted the IoT to extend its scope and expand medical services into the wireless era [1]. The results are IoT-based health-care applications, where a patient can be monitored, treated, and aided by a medical center with the use of IoT devices over the network. These applications provide many advantages for the improvement of health-care services. Some IoT-based applications in health care along with their advantages are listed in Table 1.

IoT use cases in health care

Remote patient monitoring

Remote patient monitoring (RPM) is a type of remote telehealth service that uses medical devices to observe and treat patients regardless of distance. RPM services reduce the need for patients to travel to diagnose illnesses or undergo checkups since the wireless network can achieve both [2]. Combining the

Table 1. IoT-based applications in health care along with their advantages.

Application	Advantages
Vital signs monitoring through mobile phone [6]	Wide area and scope of transmission, optimized operating system for managing data
Electronic health records reading with smart devices [7]	Portable, easy-to-learn user interface, convenient for users who already own smart devices
Wearable ECG devices [5], [8]	Low cost, compact, optimized power usage
Robots and drones for patient assistance [9]	Easy to train, have precise movements and actions, make repetitive tasks convenient, automative
Application-specific wireless sensors for emergency detection (e.g., fall prediction and pain detection) [10], [11]	Wearable, modular, can be designed to fit patient

ECG: electrocardiogram.

sensors through the wireless network creates a wireless sensor network (WSN), which is a type of IoT system that makes use of sensors that are programmed to collect data [12]. In this way, it creates a sensing network for a diverse array of raw data. Health-care services use this design to create an RPM service using the data collected from the wireless sensors. This approach complements the RPM by improving the quality of its service. The simplicity of the sensors used in the network yields faster transmission rates of collected data. As a result, the service facilitates real-time sensing and monitoring. The use of more optimized sensors to allow less energy consumption and better operation times is suggested in the article by Al Disi et al. [5]. By using simpler, application-specific sensors, RPM services can be more energy and resource efficient. The work of these authors demonstrates the advantages of using a compressed electrocardiogram (ECG) sensor to collect and deliver real-time data. This design results in an envisioned RPM service having a longer battery life due to its efficient design and lesser processing demands.

Another example of a proposed framework that uses WSNs as its RPM system is given by Catherwood et al. [13]. They have created a community-based WSN using long-range wide area network (LoRaWAN) to increase the coverage of the RPM service. With this system, they can conduct medical screenings for conditions, specifically urinary tract infections (UTIs). RPM services already benefit from being able to monitor patients over long distances. The wide area coverage of LoRaWAN and the simplicity of the WSN allow them to create a service that can span their whole community. This design shows the benefits of scalability in the use of the IoT in health care and how it improves a network's overall scope.

Smart hospitals

A smart hospital represents a type of IoT use case in health care where medical devices connect through a wireless network to improve and enhance their services. As a result, it creates an ecosystem where these devices can carry out tasks and operations related to e-health under a health-care server. As their services incorporate IoT systems, smart hospitals can improve their efficiency and lower health-care costs, as described by Catarinucci et al. [14]. With this design, monitoring and treating of patients become more self-sustaining processes since the system can automate these tasks.

A proposed solution for reducing the risks of the COVID-19 outbreak by using smart hospitals is discussed in the article of Jaiswal et al. [15]. The authors suggest that using smart technology and its properties reduces the risk of face-to-face interaction and physical contact. Instead of physically monitoring patients, a system with wireless capabilities can make use of smart devices. These services also benefit from being able to automate the monitoring process in medical treatment. A discussion of using smart hospitals to improve the quality of service that treats and cares for the elderly is provided by Maresova et al. [16]. A high percentage of hospital patients are elderly persons who suffer from conditions that impair their movement, which makes traveling more challenging. The authors suggest the use of smart technology to bring the treatment to the patient. This usage results in a patient's home becoming a part of the virtual hospital, allowing the clinic to administer adequate care to the user. Through smart computing and automation, medical centers can craft each treatment to cater to different diseases and conditions.

Mobile e-health

Mobile e-health is an IoT use case for health care that focuses more on the wireless medium that connects mobile devices for medical services [17]. Its architecture has stationary gateways in the form of fixed transceivers called *cell towers*. Each tower is a large antenna that is strategically placed over land to expand the network. Health-care services make use of this technology to extend their services over long distances.

A health-monitoring system that makes use of mobile computing is described in the work of De et al. [7]. It takes advantage of the large distances covered by a mobile network to connect patients to their health-care services. Mobile e-health allows medical services to monitor and communicate with their patients through their phones. It is beneficial in areas that only cellular networks can reach, thus ensuring that medical centers can reach their patients, especially during emergencies. Aside from its network of mobile devices, its design incorporates wireless sensors; therefore, it highlights the interchangeability of the parts of each IoT use case. These systems do not have any hard constraints, and they possess flexible architectures. This design opens the medical field to create combinations that can improve the quality of the health-care service.

Another example makes use of a 5G-based mobile network to expand its remote health-care services [17]. This design combines the mobile network with smart devices. It incorporates the automation capabilities of a smart hospital and the distance coverage of mobile e-health. Also, it highlights the advantages of each use case and the IoT as a whole when expanding remote health care and its services. These implementations of the IoT in health care are summarized in Table 2, where we highlight the domain, target IoT devices, and integrated IoT systems.

Data processing

An IoT network is a collection of devices with computing capabilities that share and exchange data within a wireless medium. In combination with a hierarchy of operations and processes, the result is a diverse set of online services. A standard network is composed of a server, a gateway, and a collection of IoT devices [18]. The server is the main control hub of the network, where most of the data are stored. The gateway is the data router of the network and serves as the bridge between the end devices and the cloud server. The end devices, or IoT devices, are the peripherals at the end of the network. In health care, these IoT devices are used to collect, transmit, and report medical data, depending on their design and purpose.

For data processing, there are three popular approaches: cloud computing, fog computing, and edge computing. The primary difference is the location at which data processing occurs. The three approaches are shown in Figure 1.

1) *Cloud-based computing*: A cloud-based IoT network concentrates all of its resources in the cloud server [11]. Most data processing is carried out in this device. The end devices are only used to collect data, which are then sent to the cloud. This centralized hierarchy allows the service to be more conveniently controlled and regulated. Also, cloud servers have an advantage in resource management because of their single control unit. Since cloud servers are considered the main online data storage of the service, data are more readily accessible from the centralized repository.
2) *Fog-based computing*: A fog-based IoT network is used to improve the network traffic by adding fog devices [6]. These fog devices function as local servers closer to the source of data. They allow the network to reallocate data packets and redirect data paths to reduce the strain on the main cloud server. The fog device takes the place of the gateway in a standard IoT setup [19]. It also extends the network in such a way that a new area of operation is added to the hierarchy, thereby allowing processes to be moved across the network.
3) *Edge-based computing*: An edge-based IoT network focuses on reallocating processing requirements to devices at the edge of the network [20]. This feature gives the IoT devices that collect the data the ability to process them as well. By doing so, analysis is readily provided to the user without the need for continuous online connection to the network [19]. Unlike the other two configurations, edge-based networks can still function effectively offline. Edge computing reduces the need for the IoT devices to continuously communicate with the main server. However, in return, this configuration requires more processing power from its IoT devices.

Devices and assistive technologies in IoT-based health care

Assistive technologies are any devices, software, or equipment that is used to aid its users in carrying out challenging tasks. In health care, these technologies can be categorized further depending on their architecture and main purpose [14]. The following sections describe examples of assistive technologies that are used in IoT-based health care. A summary of the different types of assistive technologies in IoT-based health-care services is shown in Table 3.

Wearable devices

Wearable devices are the simpler forms of assistive technology. Their purpose is to collect the designated data for which they are programmed [5]. Patients have the option to wear monitoring devices, equipped with wireless capabilities to enable RPM services, that transmit their vital signs to a configured health-care center. For instance, a wearable ECG sensor allows simultaneous monitoring of multiple patients using the same IoT network [8]. Its low power consumption gives it a long battery life. This feature improves the overall quality of service and reliability of the system. Also, the prototype sensor is cost-effective because of the simplicity of the wearable device.

This design shows the benefits of using this simple form of assistive technology. It can improve the speed of data transmitted to the server by cutting down on the preprocessing. Also, with only one parameter being monitored and no required patient–server interactions, it can be a cost-effective option for services.

Mobility and sensory aids

Mobility and sensory aids are a type of assistive technology that supports a patient by compensating for his or her disability [21]. Mobility aids focus on a person's physical aspects that pertain to motor skills. Sensory aids provide support for a patient's sensing and perceptive capabilities. Wearable devices focus on biosensing and the collection of data. Services related to these devices are usually passive in interacting with the patient. On the other hand, aiding devices provide more interactive real-time care for the patient by giving him or her proactive support.

An example of an IoT-based mobility aid is described by Saadeh et al. [10]. It is a fall-predicting/detecting system to assist patients with conditions that cause them to lack coherent motor skills. Patients such as the elderly or those under rehabilitation for trauma are susceptible to weak motor skills. This system aids them by notifying their health-care providers that

Table 2. Implementations of IoT systems in health care.

Domain	Target IoT Device(s)	IoT System(s)
Smart health-care infrastructure [14]	Biomedical systems	RPM, smart hospital
Remote health care [15]	Contact-free technologies, drones, robots	Smart hospital
Smart health care for the elderly [16]	Smart homes and furniture	Smart hospital
Real-time RPM [12]	Wireless transducer, ECG	RPM
Remote ECG monitoring, compressive sensing [5]	ECG	RPM
Community-wide UTI screening system, personalized wireless health care [13]	Android phone	RPM, mobile e-health
Mobile smart health care using 5G networks [17]	Smartphones	Smart hospital, mobile e-health
Smart neonatal health-monitoring system [7]	Vital sensors, smartphone	RPM, smart hospital, mobile e-health

they are possibly falling or have fallen. Using a support vector machine (SVM) classifier, the system can map out the movement tendencies of each patient. As a result, the system can predict and preemptively notify the health-care service that patients have fallen or become injured.

Smart devices

These are the devices that have evolved to a more diverse selection of personal devices, such as smartphones and other smart accessories [22]. A smart device is a more interactive and autonomous sensor since it contains more complex processing capabilities. As a result, assistive technologies have become more convenient for the patient without requiring specific hardware to set up. Unlike the previous two types of devices, smart devices allow most of the data processing within the device. Instead of simply collecting data and relying on the server to analyze the results, they can provide a faster diagnosis to the patient. Because of their advanced processing capabilities, they can integrate more sensors and aids into their operations.

An example of a design that uses the automation properties of smart devices is given in the work of De et al. [7]. The researchers analyzed their patient's activity through mobile device sensing paired with cloud computing. Leaning toward using smart technology to automate their services, they created a system that can cater to each patient in an organized manner and is self-sustaining. They also demonstrated the power of these intelligent sensors in creating a more responsive and adaptive system.

Challenges in IoT-based health-care services

Incorporating IoT networks in health-care services is beneficial in expanding the ability of medical centers to ensure the health of their patients. However, this integration comes with a few caveats. The following section discusses the IoT-related challenges in patient privacy, data latency, service interactability, device constraints, and scalability

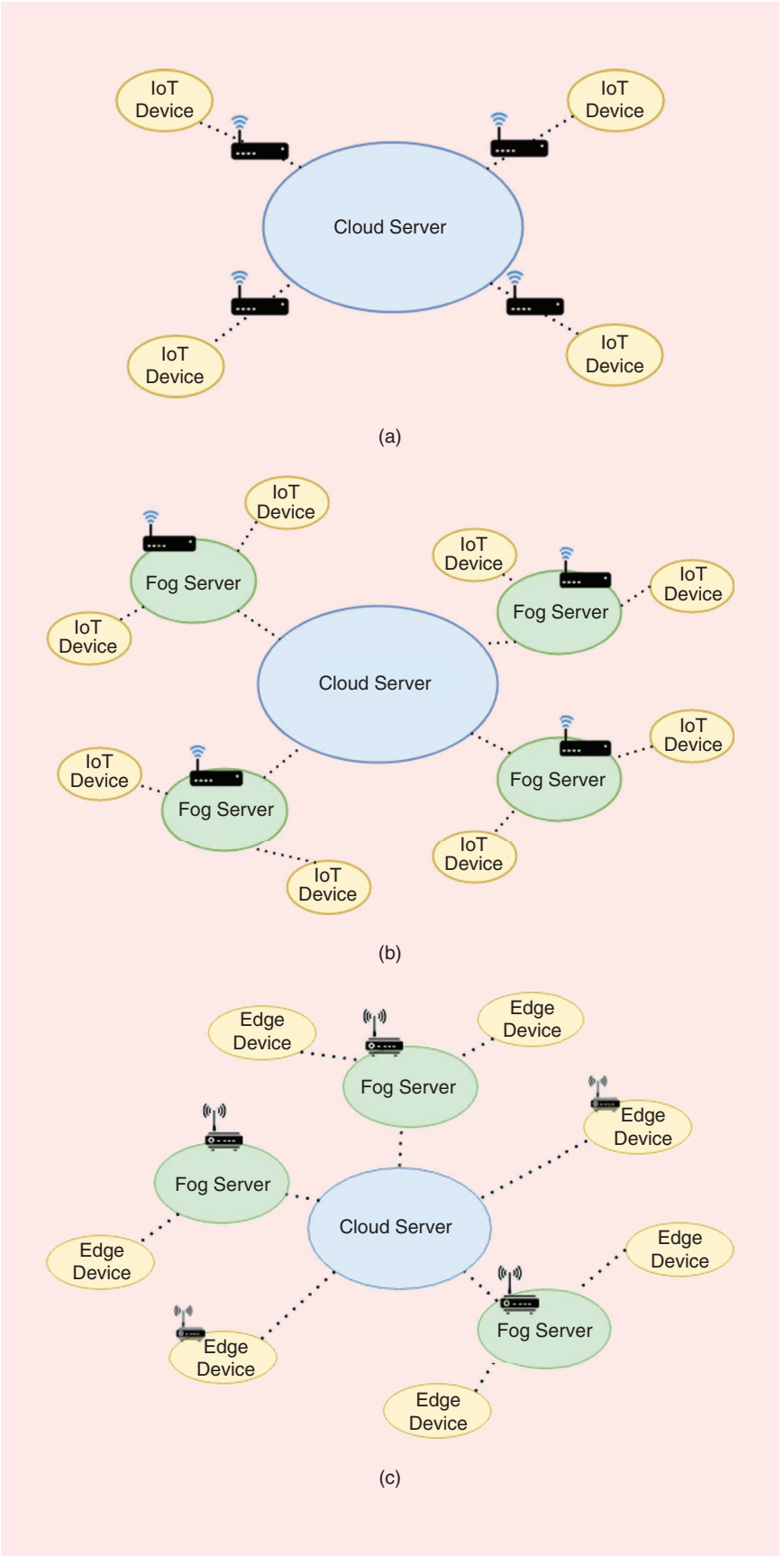

FIGURE 1. The available data processing approaches. (a) Cloud-based configuration. (b) Fog-based configuration. (c) Edge-based configuration.

in current implementations that use IoT-based health-care services.

Patient privacy

The first challenge is the security of the patient's information. The privacy of the users is important for any network-based online service [23]. Even with standard health-care service, patient confidentiality has always been advertised as a strictly valued policy. However, monitoring devices collect the patient's information through the network. This data path adds a transmission layer that is vulnerable to security attacks [4]. Also, due to the nature of wireless networks, data are being transmitted over long distances. This vulnerability exposes the data to potential security attacks. An exposed data channel could lead to patients having their personal information leaked to malicious individuals. The following are examples of security attacks that are caused by a vulnerable data channel [24]:

1) *Man-in-the-middle attack*: This type of attack occurs when an attacker modifies the transmitted data between the source and the destination. It is carried out by someone stealthily compromising the data channel and gaining access to the data being sent. These data are then tampered with and sent to their destination without triggering any suspicion from the concerned parties. Attackers can use this method to steal and modify patient information before it reaches the medical center. A visual representation of the infiltrating capabilities of this attack is shown in Figure 2(a).
2) *Spoofing*: Spoofing occurs when an attacker impersonates a compromised user. By gaining access to someone's data, the malicious individual can assume that person's identity. As a result, the attacker potentially gains access to the user's online accounts and assets. In a health-care service, an attacker can spoof an account and gain unauthorized access to and control of their records and provided service. A visual representation of the impersonating capabilities of a spoofing attack is shown in Figure 2(b).
3) *Injection*: Injection occurs when the attacker inputs wrong or modified information in place of the factual data from the user. Compromised channels are vulnerable to injected fake information that confuses services and provides misinformation. Health-care centers with vulnerable channels can result in servers receiving the wrong information. As a result, treatments can be delayed and diagnoses can be inaccurate. A visual representation of the tampering capabilities of an injection attack is shown in Figure 2(c).

Health-care centers are responsible for managing their patient's information. Compromised networks are detrimental to the quality of the service as well as the well-being of the patient [3]. As a result, people are less likely to sign up for these services if they have fears of their information being exposed to the network. Without a secure means of maintaining the privacy of their data, people will remain skeptical of IoT-based health-care services. Therefore, in an era where network security is a big concern, these services need to focus on fortifying their security to ensure their patients' data privacy.

Table 3. Examples of assistive technology in IoT-based health care.

Type	Description	Examples
Wearable devices [5], [8]	Wearable devices that are used to specifically monitor the different physiological metrics of a patient	• Electrocardiogram • Heart-rate sensor • Blood pressure sensor
Mobility and sensory aids [10], [21]	Medical devices that aid patients who are subject to motor or cognitive disabilities	• Fall sensor • Vision support • Pain sensor
Smart systems [7], [22]	Smart devices and technologies that are used to provide interactive aid for recovering and ailing patients	• GPS • Assistive robots • Smartphones

Data flow

The next challenge points to the ability of the network to maintain a consistent flow of data. IoT-based health-care services need to receive patient data at a reliable rate to be effective [12]. As a result, IoT-based health-care services incorporate wearable devices that observe their patients. These devices collect patient data and send them through the wireless network.

Another requirement for the dataflow of IoT-based health-care services is for the data to arrive in real time. This allows applications that monitor patients to be able to effectively check up on their users routinely. With a continuous influx of data from multiple devices, an IoT-based health-care service can run into issues with server overloading [22]. An example of a notable assault that could result in server overloading is a denial-of-service (DoS) attack [24]. This occurs when a server is flooded by an influx of data from multiple endpoints, with the result that the service is rendered unable to function as intended. DoS attacks are usually triggered by a malicious user. However, there are other ways to overload a server, for example, by reaching the capacity of the network. If there are too many endpoints that are transmitting data at the same time, a server will not be able to cope [18]. Without a proper way of regulating this traffic, the service will be unable to function. Therefore, to be able to combat both sources of overloading, a more reliable and adaptive medium for continuous and real-time data transport is needed.

Service interactability

Another challenge is the interactability between the service and the patient within an IoT-based health-care service. There is a lack of proper means of allowing the health-care service to interact with its patients in real time [25]. Before the incorporation of the IoT, the only option for patients was to be physically present within a medical facility to be monitored and diagnosed. Unfortunately, there are situations when the patient is not able to comply. For example, any elderly or

disabled patient is likely to have issues with continuous or long travel [26]. As a result, some doctors opt to do house visits to treat and monitor these patients. However, due to the lack of resources and an already on-demand labor force, this is no longer a valid option. Therefore, monitoring devices have been introduced to remotely monitor patients without the need for travel. However, as medical conditions become more complex, raw data are no longer enough to diagnose a patient. Patients are still required to schedule in-person checkups to allow doctors to get a full understanding of their condition. Therefore, a

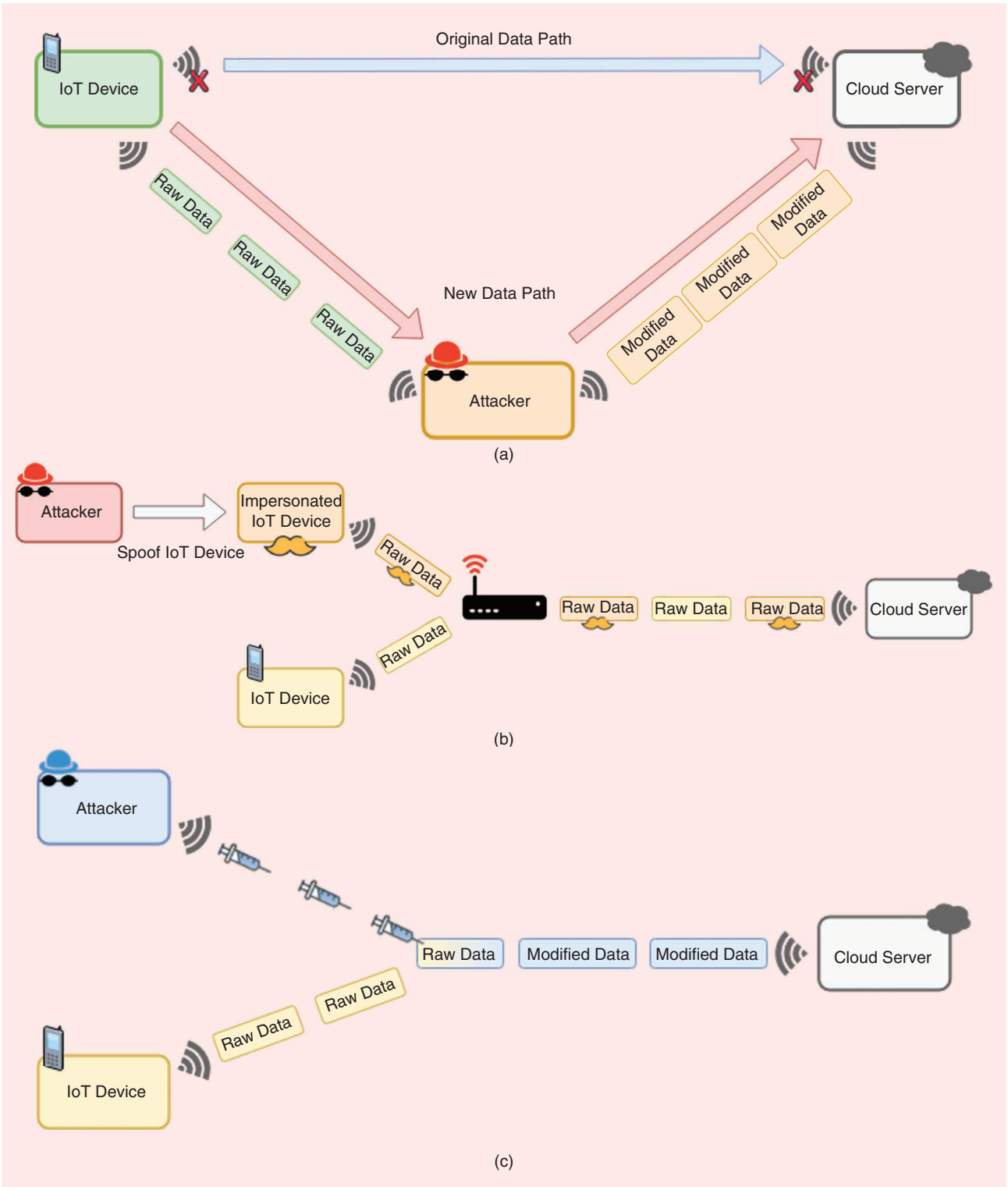

FIGURE 2. Examples of security attacks caused by a vulnerable data channel. (a) Man-in-the-middle attack. (b) Spoofing. (c) Injection.

means of being able to interact with the patient remotely will be more beneficial for the convenience of the patient [9]. By doing so, medical resources and personnel will be less hindered by distance and allocation.

As the demand for in-person checkups and treatments is reduced, health-care resources can be redirected to other patients who have more severe conditions that require full-time, in-person monitoring. However, without proper interactability, emergencies remain harder to handle within IoT-based health-care services. Without the ability to assess certain real-time situations, health-care centers will still have a difficult time providing support [11]. With service interactability, medical centers have a better grasp of the current situation of a patient. Also, data become more robust since they are properly defined in the service. With information continuously coming into the server, a means of classifying it before it is analyzed creates a more reliable system for diagnosing anomalies in a user's health. As a result, there is a higher chance of successfully diagnosing any issues or points of concern. A diagram showing the difference between having and missing service interactability in health-care services is shown in Figure 3.

Device constraints

The types of IoT devices that are used in an IoT-based health-care service pose challenges to the application based on their constraints. With the diversity of the IoT technology that is being integrated into the services, each one comes with a distinct limitation. Applications such as patient monitoring are usually implemented as long term; hence, the wearable devices are expected to remain active continuously [8]. These devices are required to operate almost indefinitely to maintain constant monitoring of the patient. As a result, they need to sustain sufficient power for long periods of time. The less frequently a device needs to replace a battery or power source, the more effective it can be at carrying out its function within the service.

Aside from the power capacity of the device, another constraint can also be from its processor [5]. With data being transmitted in a continuous and real-time manner, processors need to keep a consistent output of accurate and on-time data. Processors that fail to pass this constraint lead to the disruption of dataflow and delay of user diagnosis. This also affects the robustness and reliability of data since the arrival of information to the server is delayed [20]. This results in incoming data that are no longer accurate. Another source of inconsistent data from processors can be from the computational resource requirements of modern IoT-based health-care services [27]. This could be attributed to CPU size and processing technology limitations within the hardware. With newer services incorporating more complex calculations to improve the effectiveness of patient diagnosis and analysis, the current wearable devices are required to have some level of processing capability to keep up. However, with the growing concerns about these constraints, incremental solutions to the problem might not be enough to meet the demands for better technology.

Scalability

The last challenge that we discuss is the scalability of IoT-based health-care services [28]. One of the main reasons for incorporating the IoT in health-care services is to make data

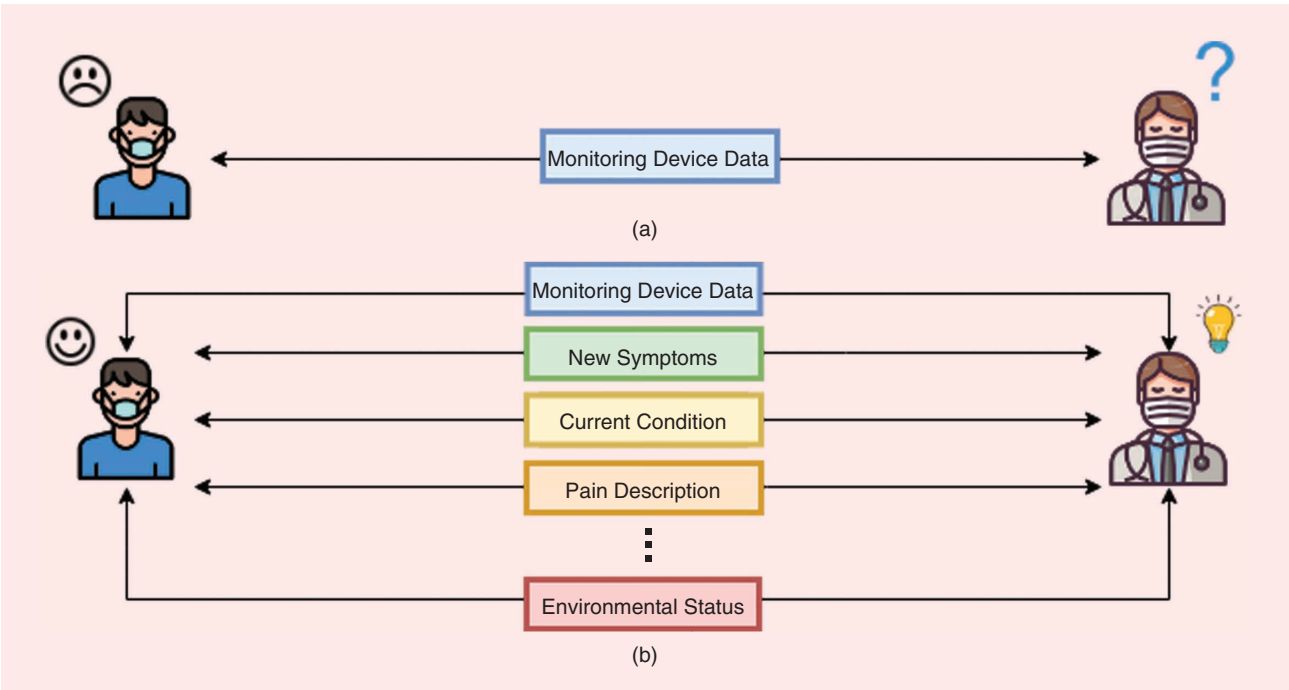

FIGURE 3. Service interactability in monitoring systems. (a) A monitoring system with no service interactability. (b) The monitoring system with service interactability.

and health-care applications more accessible to the users. As more health-care centers adapt to the paradigm shift, more devices are added to their networks. Also, as more patients transition to using IoT-based health-care services to manage their health-related records, they introduce more data to the server. Because of this influx of connecting devices, network traffic, and big data, standard IoT networks are unable to keep up [21]. This limitation is a challenge in IoT-based health-care services in terms of scalability. IoT servers that cannot manage the increasing number of connecting devices run into issues with scaling up. The result is a service that is not able to carry out its intended functionality and purpose. To be able to widen the scope of its service, the scalability of the network needs to be improved. Therefore, if health-care centers intend to increase the reach of their applications, they have to incorporate an IoT-network design that is capable of handling an increasing number of customers.

Research approaches and opportunities

The following sections highlight how challenges in patient privacy, data latency, service interactability, device constraints, and scalability can be addressed by improving the IoT medium. We also discuss some open research opportunities that ML can bring to IoT-based applications for health care.

Data filters

A critical challenge for IoT-based health-care services is patient privacy. Data are being transmitted wirelessly to a central server from multiple sources. A vulnerable network will lead to the data being compromised, which is detrimental to the privacy of the service's users. In the article by Abbas and Khan [4], the authors focus on state-of-the-art approaches related to the e-cloud health system. They highlight the capabilities of cloud computing as an environment that can relieve infrastructural tasks to a centralized unit. This unit allows the service to minimize costs while making sure that it has control over the data in the network. One of its approaches is the use of precise access control to filter the users who are allowed to access certain levels of data. By incorporating access control to every data transaction and having the permissions centralized, man-in-the-middle attacks are easier to detect, and there is more control over the data being shared between the client and the server. Instead of gaining better access control by changing the architecture, other developers suggest reinforcing what is currently implemented.

Authors Chen et al. [27] dive further into the idea of an efficient access control layer for protecting data within an RPM system. Their proposed framework uses cryptographic tools as a means to protect and filter the users who attempt to access the data within the server. These tools allow the health-care service to be protected from attackers who attempt to hack into the service and obtain patient data. The authors use data encryption as a means to hide information as it is being transmitted from the monitoring device to the server. By doing so, only trusted individuals are allowed to view and handle the data. The result is a more secure system that incorporates access control to protect the data being transmitted. Also, attackers are not able to effectively impersonate users since patient identities are more protected by the cryptographic tools used by the proposed framework.

Finally, Feng et al. [23] conducted an investigation on information disclosure as an integral component in patient privacy. By adding a feature that requires patients to permit giving access to their data, the service adds a convenient means to give users more control over their information. This willingness to disclose information on the medical platform is a crucial step in filtering data within the patient's control. It also adds a certain level of interactability within the system to entice the user. By giving patients more visible control over their information, they will feel safer in being part of the health-care service. Also, injection attacks are easier to detect since users have control over what information is allowed to enter the server. Any request for access that is not accounted for and permitted by the user can be easily filtered out. This feature allows the network to double-check the source of each data request with the patient and overcome any malicious attacks from unauthorized users.

Overall, these approaches have an underlying theme, which is the creation of a data filtering layer that filters users and their data within the server to reinforce the security of the system. Each approach shows its ability to address each type of attack that was discussed in the section "Patient Privacy." Proper data path control for the network server aids in minimizing man-in-the-middle attacks. Hiding data behind encryption and cryptographic tools allows patients to be protected from spoofing. Finally, giving more control to the users to regulate the data that they release to the server helps detect any malicious behavior that is not permitted by the patients. This allows the network to be defended from injection attacks.

Each cited solution and approach was presented as a state-of-the-art means of reinforcing the security of IoT-based health-care services. This reinforcing is done by preventing potential vulnerabilities via administrative access control, cryptographic walls, or patient consent. This creates a data filter that will serve as a gate similar to a firewall, allowing only certain types of data to flow through. In turn, data that travel through the network can be better regulated. A visual representation of the impacts of adding a data filter to the network is shown in Figure 4.

Data path control

The next challenge involves concerns about the data latency. With data being continuously transmitted from wearable devices, IoT-based health-care servers can be subject to overloading and disruptions in the flow of data. Any form of delay to the transmission of data can cause the quality of the service to diminish. As a result, these services may have bad response times to emergencies and real-time diagnoses. Al Disi et al. [5] mention the instability of a cloud-based IoT network in regulating data for online health-care services. As a result, they propose the idea of reallocating certain processes to an IoT gateway, introducing an intermediate processing unit between the end device and the cloud. They then incorporate

fog technology as a solution to allow processes to be moved within the network hierarchy.

Focusing more on the fog aspect, Verma and Sood [19] propose a similar approach. However, their proposal highlights the offloading ability of a fog server in a smart home environment. By using the distributive capabilities of a fog-based network, resources can be properly reallocated to reduce server strains. Also, fog servers can be used to implement parallelism; i.e., exact copies of an entity are used to execute the same task at the same time to increase the throughput. As the throughput is expanded, the tendency of the server to become bottlenecked by the incoming data is lessened. A visual representation of the effects of reallocation to a server overloaded with processes is shown in Figure 5.

Similar to the approach of using fog computing [19], Sood and Mahajan [6] propose a fog-based IoT framework for a decentralized blood pressure-monitoring system. The fog device allows them to move some processes closer to the local server for faster detection of emergencies. Instead of waiting for the main server to respond in case high blood pressure is detected, the local fog servers are equipped with this capability for faster detection. This feature highlights the decentralized nature of fog-based IoT networks. Decentralization allows a network to give independence to its servers. As a result, the local fog servers can function without the need to consult the main server. This freedom allows processes to be carried out faster, which helps patients receive treatment on time. Decentralization through fog servers can also reduce the number of entry points of data to the server [18]. This shift in the network hierarchy can reduce the overall amount of data being transmitted directly to the server. Partnered with the data filter that was previously discussed, a means of controlling the data path can help alleviate network strains due to potential overloading.

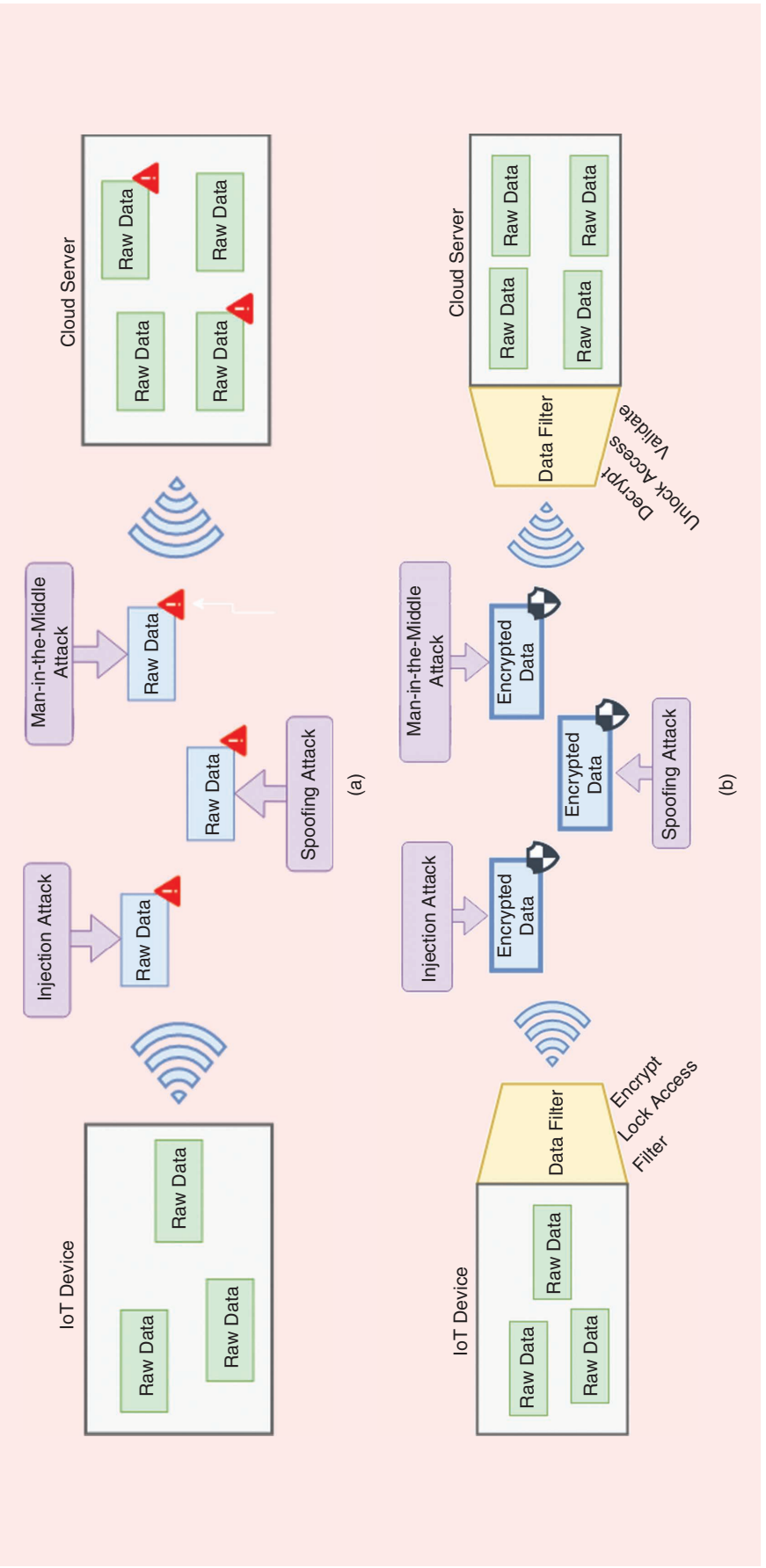

FIGURE 4. The impacts of a data filter on the security of an IoT network. (a) An IoT network without a data filter. (b) The IoT network with a data filter.

Smart interactive systems

Another challenge that we mention is service interactability. An IoT-based health-care service provides convenience to the patient in terms of distance. Also, it makes resources easier to redistribute for health-care centers. However, to improve the experience for the patients and the help that the service can provide, a more interactive system is needed. Ding and Wang [29] propose a more interactive means of bridging the medical center and the patient. By using different peripherals, such as security cameras and smart appliances, more parameters can be added to monitor a patient remotely. As a result, the system can become more adaptive and cater to a multitude of situations that the modern RPM system cannot handle. These proposed design choices will allow the health-care center to monitor the patient closely. They also eliminate the requirement to use third-party communication mediums since the embedded devices can be integrated into the service.

Yang et al. [11] have proposed an IoT-based system that increases interactability by detecting facial expressions. This model allows the service to develop automatic pain-assessment tools when monitoring patients. It shows how behavioral monitoring is also made possible with IoT networks and the peripherals that it can incorporate. Another interactive design is proposed by Mišeikis et al. [9]. They incorporate robotics to provide a therapeutic assistant that can interact with patients. This design allows remote therapy and assistance for patients with limited movement. With its technological capabilities, the design can also be used to carry out tasks such as disinfection and elevated body temperature detection.

These proposed frameworks use interactive mediums to aid the system in connecting the patient to the medical center without concerns of distance, clinical resources, or space. Instead of conducting checkups through phone calls or requiring the patients to be seen in person, these frameworks propose a smart interactive means of administering medical care for patients using IoT-based health-care services. This will be especially useful for future events, similar to the recent COVID-19 pandemic, where health-care centers are being overloaded and people are required to stay indoors. This design creates a smarter health-care service that provides patients who are not able to travel for checkups with the ability to seek medical help. It also lets clinics that have capacity and resource issues to be able to take in patients without pushing them into queues and waiting lists. Overall, these designs open the possibility for health-care centers to expand their IoT-based services, allowing them to treat a larger number of patients.

Smartphones and parallel programming

The next challenge arises from the constraints found within the IoT devices. Restrictions such as power consumption and processor capabilities limit the progress of IoT-based health-care services. Instead of designing a new wearable device every time a change is needed, some approaches have moved to incorporate other available technologies instead, for example, smartphones. These devices can be equipped with

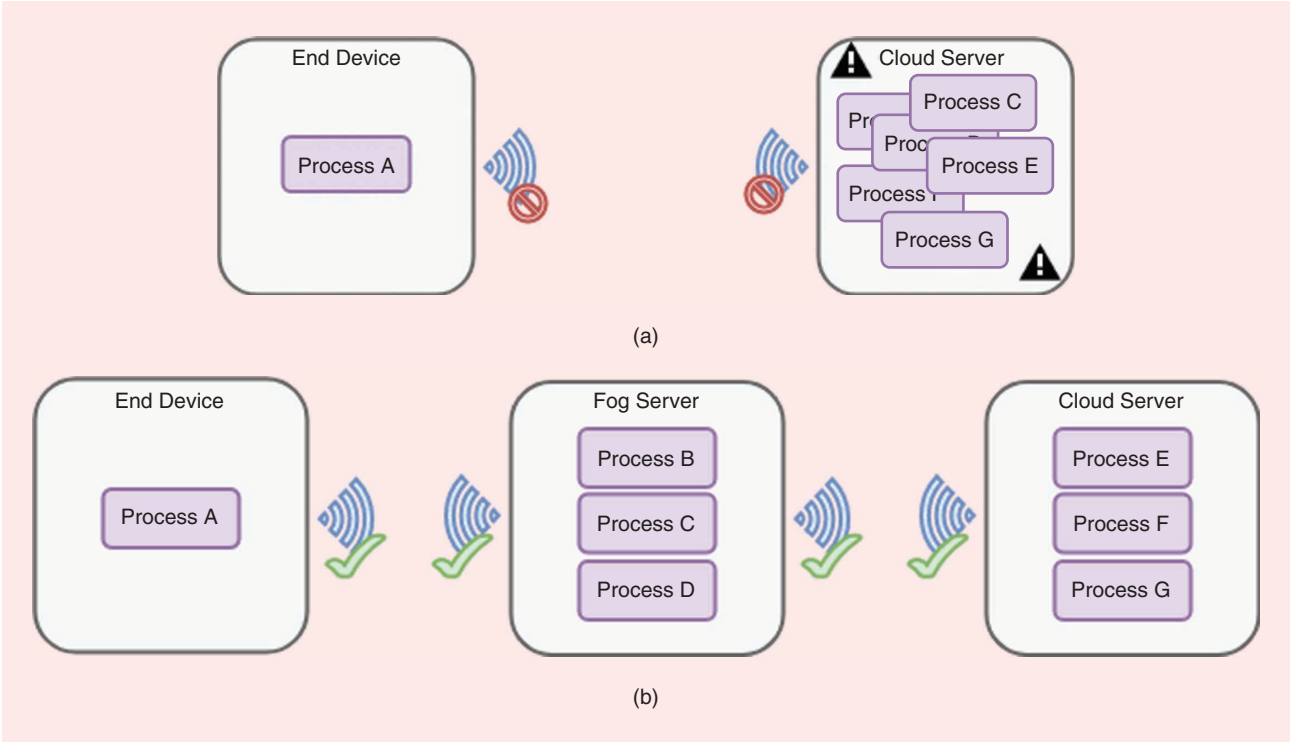

FIGURE 5. The reallocative properties of adding a fog server to the network. (a) A cloud network overloaded by processes. (b) A fog network with reallocated processes.

sensors that allow the collection of health-based metrics. In the article by Guo [30], the author takes advantage of the capabilities of smartphones by designing an attachable dongle for biosensing. With the smartphone, power consumption is less of an issue because of its already-efficient design. Also, by using ultralow consumption sensors, the overall battery life of the phone is not impacted. Meanwhile, by using the smartphone's processor to analyze the collected data, the sensor no longer needs a high-end one. This design minimizes the constraints of power consumption and processing power by taking advantage of the already-advanced design of the smartphone.

Smart and adaptive environments

The final challenge that we highlight is scalability. With the increase of devices that are using IoT-based health-care services, growing networks become harder to manage. To improve the state of an IoT network to handle this challenge, a more adaptive environment is needed. Sun et al. [31] discuss the increase in big data sources, such as health care and safety. They propose to use smart cities and connected communities to manage this influx of data and devices. By introducing a smart environment where IoT devices can be connected wirelessly, data and processes can be shared effectively. Also, by using the smart capabilities of the network, it can be made adaptive to the devices that connect to each implemented health-care service.

Zhang et al. [28] have proposed the use of ubiquitous WSNs to create a more standardized network of sensing devices for IoT-based health-care services to use. This allows the incorporation of a wide variety of sensors that together are capable of real-time technical sensing. With the network able to increase its scope through the incorporation of ubiquitous WSNs, handling the increase of users is less of a challenge. When partnered with smart environments, regulating the influx of devices is attainable through the network's adaptive architecture. Further investment toward an adaptive medium results in the incorporation of automative technologies, such as blockchains and deep learning.

Kumar et al. [32] propose a design using blockchain technology to improve the management of health records within a health-care service. With the use of smart contracts, it can automate the management of access control for each device. Partnered with the distributive nature of blockchains, the regulation of resources within the network is made more efficient and effective. Overall, these cited state-of-the-art solutions show the capabilities of technologies, such as smart environments partnered with deep learning and blockchains, in improving the scalability of IoT-based health-care services. With the use of their automative and adaptive features, each creates an environment that can serve as the main administrator of the devices within the IoT network.

ML opportunities in health care

In conjunction with the idea of providing a smarter interactive system, another approach in solving service interactability could be from the incorporation of ML techniques and neural networks. ML is a learning tool that uses collected data and establishes trends through training and system modeling. With these behavioral models, results from similar events can be inferred or predicted. The usage of ML via SVMs and an adaptive-network-based fuzzy inference system model to create an IoT-based smart health monitoring and surveillance framework for COVID-19 risk exposure detection has been proposed [33]. With the use of these analytic ML techniques to train the model, the framework can monitor a registered patient and his/her physical condition. Also, with the infection data that the framework has collected and trained with, it can notify the patient of any risks and direct him/her toward proper social distancing. The model claims the ability to regulate the safety of their patients through a smart wearable armband. It also helps alert those around them to make sure that the spread of the virus is minimized. This framework shows the potential of ML to model the trends of health-based data, and, with the use of IoT networks, it can improve the safety and care of each patient.

A deep learning approach is proposed in the article by Amin et al. [34]. By using two convolutional neural network models, they were able to detect and classify pathological behavior within electroencephalogram readings. This model serves as a cognitive system that is capable of improving the quality and effectiveness of the detecting service for the patient. Also, with the use of analytic tools, such as ML and neural networks, data can be used to refine the overall diagnosing experience within health-care services.

Conclusions

Incorporating IoT devices and assistive technologies in health-care services has several advantages, poses unique challenges, and creates new research opportunities. The issues regarding patient privacy, dataflow, service interactability, device constraints, and scalability are discussed in this article. Related implementations and frameworks have been investigated to discover improvements to IoT networks addressing these issues. The use of ML techniques has also been proposed to improve the effectiveness of the health-care services provided to patients. As a result, faster responses to address risks and emergencies are made possible. Instead of having a cloud server decide if the data warrant any action, smart wearable devices can now detect anomalies and emergencies earlier by moving the decision layer closer to the patient. In addition, robotics, smart appliances, ML, and neural networks can be used to assist ailing patients as they are monitored. Overall, IoT devices provide a window to more secure, efficient, and interactive systems. Their capabilities will open more opportunities for researching and developing health-care services to cater to the evolving medical technology.

Authors

Marc Jayson Baucas (baucas@uoguelph.ca) received his B.Eng. degree (2018) in computer engineering and his

M.A.Sc. degree (2019) in engineering systems and computing from the University of Guelph, Ontario, Canada. He is currently working toward completing his Ph.D. degree at the University of Guelph, Guelph, Ontario, N1G 2W1, Canada. His research interest is in security in the Internet of Things (IoT) with a focus on e-health, wearable IoT devices, and blockchain technology. He is a Student Member of IEEE.

Petros Spachos (petros@uoguelph.ca) received his diploma degree in electronic and computer engineering from the Technical University of Crete, Greece, and his M.A.Sc. and Ph.D. degrees, both in electrical and computer engineering, from the University of Toronto, N1G 2W1, Canada. He is an associate professor at the School of Engineering, University of Guelph, Guelph, Ontario, Canada. His research interests include experimental wireless networking and mobile computing with a focus on wireless sensor networks, smart cities, and the Internet of Things. He is a Senior Member of IEEE.

Stefano Gregori (sgregori@uoguelph.ca) received his Laurea and Ph.D. degrees in electrical and computer engineering from the University of Pavia, Pavia, Italy. He is currently a professor of computer engineering at the University of Guelph, Guelph, Ontario, N1G 2W1, Canada. His research interests include the design, analysis, and characterization of integrated circuits with analog and digital applications, integrated power converters, and sensor interfaces. He is a Senior Member of IEEE.

References

[1] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, June 2015. doi: 10.1109/ACCESS.2015.2437951.

[2] B. Hassan, R. Ahmed, B. Li, and O. Hassan, "An imperceptible medical image watermarking framework for automated diagnosis of retinal pathologies in an ehealth arrangement," *IEEE Access*, vol. 7, pp. 69,758–69,775, June 2019. doi: 10.1109/ACCESS.2019.2919381.

[3] M. Shuai, L. Xiong, C. Wang, and N. Yu, "Lightweight and privacy-preserving authentication scheme with the resilience of desynchronisation attacks for WBANs," *IET Inform. Security*, vol. 14, no. 4, pp. 380–390, July 2020. doi: 10.1049/iet-ifs.2019.0491.

[4] A. Abbas and S. U. Khan, "A review on the state-of-the-art privacy-preserving approaches in the e-Health clouds," *IEEE J. Biomed. Health Inform.*, vol. 18, no. 4, pp. 1431–1441, July 2014, doi: 10.1109/JBHI.2014.2300846.

[5] M. Al Disi et al., "ECG signal reconstruction on the IoT-gateway and efficacy of compressive sensing under real-time constraints," *IEEE Access*, vol. 6, pp. 69,130–69,140, Dec. 2018. doi: 10.1109/ACCESS.2018.2877679.

[6] S. K. Sood and I. Mahajan, "IoT-fog-based healthcare framework to identify and control hypertension attack," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1920–1927, Apr. 2019. doi: 10.1109/JIOT.2018.2871630.

[7] D. De, A. Mukherjee, A. Sau, and I. Bhakta, "Design of smart neonatal health monitoring system using SMCC," *Healthcare Technol. Lett.*, vol. 4, no. 1, pp. 13–19, Nov. 2017. doi: 10.1049/htl.2016.0054.

[8] E. Spanò, S. Di Pascoli, and G. Iannaccone, "Low-power wearable ECG monitoring system for multiple-patient remote monitoring," *IEEE Sensors J.*, vol. 16, no. 13, pp. 5452–5462, July 2016. doi: 10.1109/JSEN.2016.2564995.

[9] J. Mišeikis et al., "Lio—A personal robot assistant for human–robot interaction and care applications," *IEEE Robot. Automat. Lett.*, vol. 5, no. 4, pp. 5339–5346, Oct. 2020. doi: 10.1109/LRA.2020.3007462.

[10] W. Saadeh, S. A. Butt, and M. A. B. Altaf, "A patient-specific single sensor IoT-based wearable fall prediction and detection system," *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 27, no. 5, pp. 995–1003, May 2019. doi: 10.1109/TNSRE.2019.2911602.

[11] G. Yang et al., "IoT-based remote pain monitoring system: From device to cloud platform," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 6, pp. 1711–1719, Nov. 2018. doi: 10.1109/JBHI.2017.2776351.

[12] Y. Yang, X. Zhu, K. Ma, R. B. V. B. Simorangkir, N. C. Karmakar, and K. P. Esselle, "Development of wireless transducer for real-time remote patient monitoring," *IEEE Sensors J.*, vol. 16, no. 12, pp. 4669–4670, June 2016. doi: 10.1109/JSEN.2016.2553360.

[13] P. A. Catherwood, D. Steele, M. Little, S. Mccomb, and J. Mclaughlin, "A community-based IoT personalized wireless healthcare solution trial," *IEEE J. Transl. Eng. Health Med.*, vol. 6, pp. 1–13, May 2018. doi: 10.1109/JTEHM.2018.2822302.

[14] L. Catarinucci et al., "An IoT-aware architecture for smart healthcare systems," *IEEE Internet Things J.*, vol. 2, no. 6, pp. 515–526, Dec. 2015. doi: 10.1109/JIOT.2015.2417684.

[15] R. Jaiswal, A. Agarwal, and R. Negi, "Smart solution for reducing the COVID-19 risk using smart city technology," *IET Smart Cities*, vol. 2, no. 2, pp. 82–88, July 2020. doi: 10.1049/iet-smc.2020.0043.

[16] P. Maresova et al., "Health-related ICT solutions of smart environments for elderly-systematic review," *IEEE Access*, vol. 8, pp. 54,574–54,600, Mar. 2020. doi: 10.1109/ACCESS.2020.2981315.

[17] A. Ahad, M. Tahir, and K. A. Yau, "5G-based smart healthcare network: Architecture, taxonomy, challenges and future research directions," *IEEE Access*, vol. 7, pp. 100,747–100,762, Aug. 2019. doi: 10.1109/ACCESS.2019.2930628.

[18] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing fog computing for Internet of Things applications: Challenges and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 601–628, First quarter 2018. doi: 10.1109/COMST.2017.2762345.

[19] P. Verma and S. K. Sood, "Fog assisted-IoT enabled patient health monitoring in smart homes," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1789–1796, June 2018. doi: 10.1109/JIOT.2018.2803201.

[20] Y. Deng, Z. Chen, X. Yao, S. Hassan, and A. M. A. Ibrahim, "Parallel offloading in green and sustainable mobile edge computing for delay-constrained IoT system," *IEEE Trans. Veh. Technol.*, vol. 68, no. 12, pp. 12,202–12,214, Dec. 2019. doi: 10.1109/TVT.2019.2944926.

[21] E. Mezghani, E. Exposito, and K. Drira, "A model-driven methodology for the design of autonomic and cognitive IoT-based systems: Application to healthcare," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 1, no. 3, pp. 224–234, June 2017. doi: 10.1109/TETCI.2017.2699218.

[22] N. Alshurafa et al., "Improving compliance in remote healthcare systems through smartphone battery optimization," *IEEE J. Biomed. Health Inform.*, vol. 19, no. 1, pp. 57–63, Jan. 2015. doi: 10.1109/JBHI.2014.2329712.

[23] C. Feng, Z. Cheng, and L. Huang, "An investigation into patient privacy disclosure in online medical platforms," *IEEE Access*, vol. 7, pp. 29,085–29,095, Mar. 2019. doi: 10.1109/ACCESS.2019.2899343.

[24] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sept. 2016. doi: 10.1109/JPROC.2016.2558521.

[25] A. Ara, M. Al-Rodhaan, Y. Tian, and A. Al-Dhelaan, "A secure privacy-preserving data aggregation scheme based on bilinear ElGamal cryptosystem for remote health monitoring systems," *IEEE Access*, vol. 5, pp. 12,601–12,617, July 2017. doi: 10.1109/ACCESS.2017.2716439.

[26] D. Niyato, E. Hossain, and S. Camorlinga, "Remote patient monitoring service using heterogeneous wireless access networks: Architecture and optimization," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 412–423, May 2009. doi: 10.1109/JSAC.2009.090506.

[27] Y. Chen, W. Sun, N. Zhang, Q. Zheng, W. Lou, and Y. T. Hou, "Towards efficient fine-grained access control and trustworthy data processing for remote monitoring services in IoT," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 7, pp. 1830–1842, July 2019. doi: 10.1109/TIFS.2018.2885287.

[28] Y. Zhang, L. Sun, H. Song, and X. Cao, "Ubiquitous WSN for healthcare: Recent advances and future prospects," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 311–318, Aug. 2014. doi: 10.1109/JIOT.2014.2329462.

[29] S. Ding and X. Wang, "Medical remote monitoring of multiple physiological parameters based on wireless embedded internet," *IEEE Access*, vol. 8, pp. 78,279–78,292, May 2020. doi: 10.1109/ACCESS.2020.2990167.

[30] J. Guo, "Smartphone-powered electrochemical biosensing dongle for emerging medical IoTs application," *IEEE Trans. Ind. Inf.*, vol. 14, no. 6, pp. 2592–2597, June 2018. doi: 10.1109/TII.2017.2777145.

[31] Y. Sun, H. Song, A. J. Jara, and R. Bie, "Internet of Things and big data analytics for smart and connected communities," *IEEE Access*, vol. 4, pp. 766–773, Mar. 2016. doi: 10.1109/ACCESS.2016.2529723.

[32] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, and E. Hossain, "A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes," *IEEE Access*, vol. 8, pp. 118,433–118,471, July 2020. doi: 10.1109/ACCESS.2020.3004790.

[33] S. S. Vedaei et al., "COVID-SAFE: An IoT-based system for automated health monitoring and surveillance in post-pandemic life," *IEEE Access*, vol. 8, pp. 188,538–188,551, Oct. 2020. doi: 10.1109/ACCESS.2020.3030194.

[34] S. U. Amin, M. S. Hossain, G. Muhammad, M. Alhussein, and M. A. Rahman, "Cognitive smart healthcare for pathology detection and monitoring," *IEEE Access*, vol. 7, pp. 10,745–10,753, Jan. 2019. doi: 10.1109/ACCESS.2019.2891390.

SP