Journal of Network and Computer Applications 192 (2021) 103164

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

A systematic review of IoT in healthcare: Applications, techniques, and trends

Mostafa Haghi Kashani [a], Mona Madanipour [b], Mohammad Nikravan [a], Parvaneh Asghari [c], Ebrahim Mahdipour [b,*]

[a] Department of Computer Engineering, Shahr-e-Qods Branch, Islamic Azad University, Tehran, Iran
[b] Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran
[c] Department of Computer Engineering, Central Tehran Branch, Islamic Azad University, Tehran, Iran

ARTICLE INFO

Keywords:
Internet of things (IoT)
Healthcare
e-health
Systematic review

ABSTRACT

Internet of Things (IoT) is an ever-expanding ecosystem that integrates software, hardware, physical objects, and computing devices to communicate, collect, and exchange data. The IoT provides a seamless platform to facilitate interactions between humans and a variety of physical and virtual things, including personalized healthcare domains. Lack of access to medical resources, growth of the elderly population with chronic diseases and their needs for remote monitoring, an increase in medical costs, and the desire for telemedicine in developing countries, make the IoT an interesting subject in healthcare systems. The IoT has a potential to decrease the strain on sanitary systems besides providing tailored health services to improve the quality of life. Therefore, this paper aims to identify, compare systematically, and classify existing investigations taxonomically in the Healthcare IoT (HIoT) systems by reviewing 146 articles between 2015 and 2020. Additionally, we present a comprehensive taxonomy in the HIoT, analyze the articles technically, and classify them into five categories, including sensor-based, resource-based, communication-based, application-based, and security-based approaches. Furthermore, the benefits and limitations of the selected methods, with a comprehensive comparison in terms of evaluation techniques, evaluation tools, and evaluation metrics, are included. Finally, based on the reviewed studies, power management, trust and privacy, fog computing, and resource management as leading open issues; tactile Internet, social networks, big data analytics, SDN/NFV, Internet of nano things, and blockchain as important future trends; and interoperability, real-testbed implementation, scalability, and mobility as challenges are worth more studying and researching in HIoT systems.

1. Introduction

Today's world has been involved with many challenges related to public health issues of chronic diseases due to threatening infections such as COVID-19. The rise in health problems along with high healthcare costs encourage everyone, especially elderly and disabled people, to use remote health management via computer-aided technologies (Garg et al., 2020), (Hosseinzadehet al., 2020a). In recent years, the Internet of Things (IoT), as a network of connected devices that interact with one another, plays an important role in enabling automation in many fields such as remote and smart healthcare systems. Technologically, the IoT consists of some popular technologies such as wireless body area networks (WBANs), wireless sensor networks (WSNs) (Mainetti et al., 2011), and radio frequency identification (RFID) to transfer the obtained data to the cloud for analyzing and extracting meaningful data for on-time proper decision making (Al-Fuqaha et al., 2015), (Asghari et al., 2019a), (Baker et al., 2017). With a rise in the desire to make healthcare more personalized, proactive, and cost-effective, the IoT can be considered and employed as a significant technology in health management systems (e.g., mental health and global pandemic (COVID19)) (Garg et al., 2020), (Al-Fuqaha et al., 2015). In this regard, the implementation of IoT in healthcare can be classified into three parts (Tsiounia et al., 2019): i) tracing people and other objects (staff, medical teams, and patients), ii) people authentication and identification, and iii) automatic data sensing and collection. For example, the IoT provides health monitoring anytime and anywhere around the human body with

* Corresponding author.
E-mail addresses: mh.kashani@qodsiau.ac.ir (M. Haghi Kashani), mona.madanipour@srbiau.ac.ir (M. Madanipour), m.nikravan@qodsiau.ac.ir (M. Nikravan), p_asghari@iauctb.ac.ir (P. Asghari), mahdipour@srbiau.ac.ir (E. Mahdipour).

https://doi.org/10.1016/j.jnca.2021.103164
Received 4 January 2021; Received in revised form 13 May 2021; Accepted 7 July 2021
Available online 22 July 2021

WBAN technology, and can prevent from hospital infections, emergencies management, and post-discharge care. Therefore, the IoT completely redefines devices, applications, and people in the healthcare domain (Habibzadeh et al., 2020), (Atzori et al., 2010).

Henceforward, healthcare environments can be extensively revolutionized by the use of IoT opportunities such as the Internet of Medical Things (IoMT) technology that includes connected medical sensors or special medical devices to provide a personalized approach to healthcare delivery (Gatouillat et al., 2018). The use of IoMT technology in healthcare systems, called Healthcare Internet of Things (HIoT) creates appropriate therapeutic strategies for patients by connecting medical devices to the Internet and carrying out various telehealth services such as the supervision of elderlies, telemonitoring, teleconsultations, and computer-assisted rehabilitation. In most articles, the terms IoMT and HIoT have been applied as alternatives for the integration of medical devices and applications that can be connected to health care information technology systems in an IoT-based environment (Habibzadeh et al., 2020). On the other hand, the convergence of big data and IoT is a new concept in sanitary systems that leads to smart management of the healthcare processes (Lu and Liu, 2011), (Karimi et al., 2021). Big data analytics has enabled prescriptive, autonomous, and predictive analysis of healthcare approaches. To this end, personalized healthcare enables remote monitoring of patients, diagnosis, early detection, and diseases prevention, especially chronic diseases such as diabetes, obstructive pulmonary disease, cancer, arthritis, and heart disease (Lloret et al., 2017).

To date, a comprehensive systematic literature review (SLR) of research on HIoT that specifies the advance in general and identifies research questions, trends, and future directions of HIoT in particular has rarely been conducted. With the increasing desire for IoT in healthcare, exploring a study scheme for HIoT systems is necessary. A systematic review identifies, categorizes, and synthesizes a comparative method of investigation and leads to knowledge transfer in research associations. To this end, we aim to answer the following research questions (RQs) by reviewing the existing studies:

- What are the major practical motivations behind associating IoT in healthcare systems?
- What research scopes exist in IoT-based healthcare systems? Besides, what achievements are there in this area?
- What are the existing techniques and approaches that enable IoT in healthcare systems?
- What are the existing open issues, future trends, and key challenges in HIoT? And what research directions should form in HIoT systems in the future?

We followed guidelines in (Brereton et al., 2007), (KitchenhamKeele, 2004) to conduct an SLR with the aim of *identification, classification, and systematic comparison of the existing studies concentrating on IoT in healthcare*. In other words, this study intends to present, systematically identify, and taxonomically classify the investigations on HIoT that leads to providing an exhaustive comparison with the analysis of limitations and potentials of the current papers. This review presents a systematic review of the recent researches focusing on applied techniques, methods, and tools in HIoT. Therefore, to determine the need for improving HIoT systems and introducing open issues and future trends, 146 studies are selected, categorized, and compared.

Here, the current study strategies, techniques, methods, best experiences, and practices used in HIoT are investigated. Additionally, this paper shows that studies in HIoT are growing rapidly and recognizes the need for using IoT in healthcare systems. In this regard, the outcomes of this SLR are impressive for the following cases:

- Researchers in IoT and modern healthcare who need exploration of the related studies
- Medical field experts interested in realizing the current methods, strategies, techniques, and tools with the existing constraints in HIoT systems

The rest of this paper is organized as Fig. 1: Section 2 describes the background, and Section 3 explains the related reviews and surveys in HIoT. Section 4 provides the research methodology, and Section 5 presents a taxonomy of the selected approaches and compares their features. In Section 6, the analysis of the results is discussed. In addition, Section 7 discusses open issues and future trends. Threats to validity and limitations are presented in Section 8, and finally, the conclusion is included in Section 9. Fig. 2 illustrates a reading map, so readers who are interested in IoT and healthcare can focus on Sections 1, 2, 3, 7, and 9. Sections 1, 5.1, 6, 7, and 9 are for those who would like to gain information about sensor management in HIoT, and Sections 1, 5.2, 6, 7, and 9 are interesting for resource management. Communication management comes in detail in Sections 1, 5.3, 6, 7, and 9. Application management is explored in Sections 1, 5.4, 6, 7, and 9. Finally, we recommend Sections 1, 5.5, 6, 7, and 9 to readers who are interested in gaining an overview of the security management in HIoT.

2. Background

In this section, a brief definition of IoT and healthcare is presented. At first, an outline of IoT and healthcare is explained. Then, the layered architecture of HIoT is described. Finally, the important metrics that are used in this subject are defined.

2.1. Internet of things

The term IoT was defined by Ashton (2009) in the supply management area for the first time in 1999. Nowadays, different definitions of the IoT can be addressed, such as a sophisticated network of addressable and identifiable things uniquely. These things connect to servers to transfer their data and extract valuable knowledge that efficiently provides appropriate services. In other words, the IoT consists of innumerable devices and objects, including various types of sensors and actuators, that connect and interact with each other through the Internet (Nikravan et al., 2011), (Atzori et al., 2010), (Najafizadeh and Kashani, 2011).

In addition, a typical IoT environment consists of communication interfaces, sensors, advanced algorithms, and cloud interfaces. Sensors are responsible for collecting data from various devices. Also, RFID technologies and WSN provide network and communication infrastructures (Fosso Wamba et al., 2013); advanced algorithms are used to analyze and process data. Numerous client/server requests can be exchanged in the cloud environment and allow the users to have access various types of services simultaneously (Asghari et al., 2019a), (Sultan, 2014). Due to cloud computing challenges such as latency, reliability, resource constraints, etc., fog computing is generated to overcome these limitations and run the same applications anywhere close to users with real-time analysis and efficient decision-making features (Farahani et al., 2018), (Sheikh Sofla et al., 2021).

Despite all improvements in IoT, this new paradigm is still in its infancy and has many research topics in various issues such as standardization, heterogeneity of different devices, scalability, security, privacy, and so forth. In this regard, interoperability among smart devices to communicate and interconnect heterogeneous devices and different vendor systems, which is easy to implement and cost-effective, is a particular issue (Jabbar et al., 2017). In addition, low-cost interoperability among smart objects is an essential aspect for IoT helping clients to continue working with different vendors in the near future. Finally, the IoT can reduce the cost of buildings, solve the complexity of organization infrastructures, and help support heterogeneous infrastructures (Ullah et al., 2017), (Najafizadeh et al., 2021).

Nowadays, the IoT paradigm covers various applications such as

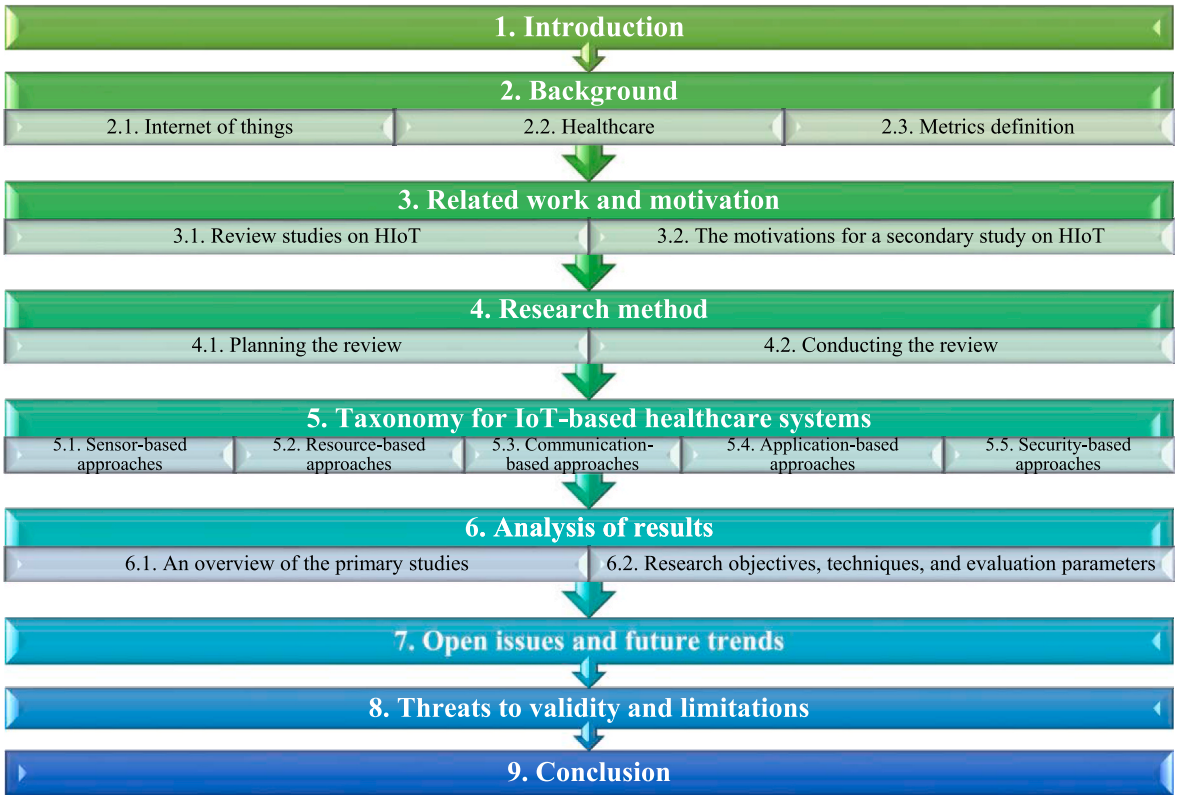

Fig. 1. The structure of our study.

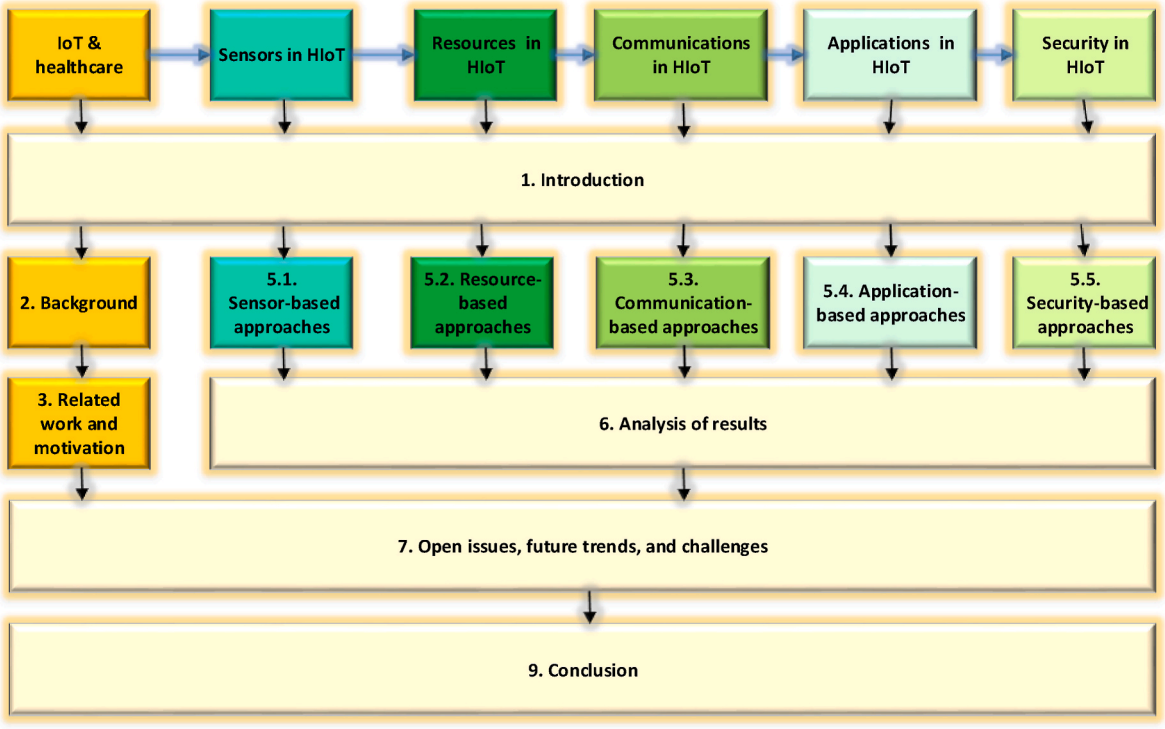

Fig. 2. A reading map for IoT and healthcare.

transport, smart cities, monitoring, healthcare, etc. Despite the heterogeneity of IoT devices, the data in IoT applications such as smart cities and smart homes are easily correlated, combined, and compared to be adapted to people's needs. For example, in the healthcare industry, with the emergence of the IoT paradigm, sanitary systems can be revolutionized by this technology. It can play an important role in telemonitoring at the hospital, especially at home for elderlies with chronic diseases. By using this technology, in the future, healthcare systems will experience major effects such as reduction of response time to detect anomalies, high-quality care, low hospitalization costs, and high life expectancy (Sakiz and Sen, 2017), (Ray et al., 2019a).

2.2. Healthcare

Given the current state of the world and the spread of the epidemic and infectious diseases such as COVID-19, along with other reasons related to this pandemic such as high cost, long-distance, and the need for quarantine in this critical period of time, going to medical centers is difficult and sometimes impossible for some (Singh et al., 2020), (Mohammed et al., 2020), (Kaur and Sharma, 2020) especially for the elderly and disabled ones most of whom suffer from at least one chronic disease. Therefore, a convenient, extensive, and computer-aided technology is crucial to satisfy the needs for long-term caring and remote medical monitoring to provide an appropriate quality of life for patients and to reduce the financial burden (Marengoniet al., 2011), (Nasajpour et al., 2020).

IoT has revolutionized the sanitary system by analyzing big data and has developed it into a predictive and intelligent system by connecting many IoT devices to capture real-time physiological data of patients such as glucose levels in the blood, temperature monitors, and other required data. The main goal is to provide novel medical services for patients, such as early detection of diseases and continuous monitoring of serious ones. Indeed, the IoT can help the healthcare industry in such cases as preventative care, disease management, assisted living, and clinical monitoring remotely. Furthermore, the most common IoT applications in healthcare are in some areas such as home healthcare, mobile healthcare or e-healthcare, hospital management, and etc. (Ahmadi et al., 2018), (Dey et al., 2018). Finally, the convergence of IoT and healthcare systems has enabled smart management of the healthcare processes, self-caring, detection of some events such as seizure detection, fall detection to help Parkinson's gait disturbance, stroke rehabilitation, neurologic monitoring, and cardiac to reduce medication and human errors. However, more challenges still exist to achieve effective and secure healthcare applications such as self-improvement, self-learning, and hardware systems (e.g., implantable sensors and wearables), privacy, security, and standardization. Today, there are various security protocols to protect data from attacks or threats, including authentication, and encryption techniques, public-key cryptosystems, k-anonymity, etc. (Wilson, 2017), (Ahmed et al., 2018).

According to Fig. 3, the HIoT system has a well-known classic four-layer architecture, including the perception layer, networking layer, middleware layer, and application/business layer, which is illustrated in Fig. 3 (Qi et al., 2017). The explanations of the layers are as follows (Ashton, 2009), (Qi et al., 2017), (Wu et al., 2010), (Vilela et al., 2019):

- *Perception layer*: This layer is at the bottom of the other layers that can be attended as the physical or hardware layer. Data collection and signaling are performed in this layer, then prepared data will be sent to the network layer.
- *Network layer*: This layer aims to connect all smart devices together and allow them to transfer health data and exchange among themselves. This layer transmits the health data securely from patients to the base station via Zigbee, Bluetooth, infrared, Wi-Fi technologies, and so on.
- *Middleware layer*: This layer includes service with its requester related to names and addresses. The HIoT application programmers can work with non-homogeneous objects with no attention to a specific equipment platform. Health data is gathered from the network layer and stored in a database via this layer.
- *Application/Business layer*: This layer procures healthcare services that evaluate and integrate the data received from other layers. This layer can provide high-quality healthcare services to satisfy patients' requests. The achievements of HIoT systems will rely on the importance of applied innovations, technologies, and proper business models; therefore, this layer is responsible for managing all activities and healthcare services through creating graphs, business models, and flowcharts.

Also, three major steps, including i) data generation, ii) data processing, and iii) information consuming, can be considered as three main phases of a workflow in a general healthcare system constructed in an IoT-based architecture which is known as HIoT systems. The mentioned phases are described as follows:

i) *Data generation:* Data generation phase comprises collecting and generating the needed data by various sensors, medical devices, and even direct data entry by patients or involved healthcare teams. This phase is performed through the perception layer, and the collected data is transferred via the network layer.
ii) *Data processing:* Data processing phase implies the analysis of generated data through some well-known mechanisms such as machine learning methods by means of data analysis tools. This phase is performed through the middleware layer.

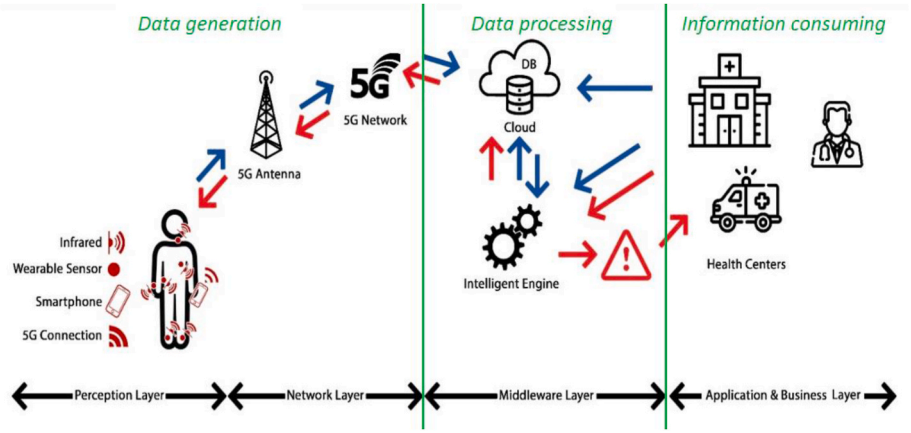

Fig. 3. The architecture of IoT in healthcare systems (Ashton, 2009), (Vilela et al., 2019).

iii) *Information consuming*: The outcomes and analytics of the data processing phase can be used in the information consuming phase for any required decision-making performed by medical teams for patients, and even this analytical information can be used for activating the actuators. This phase is performed through the application and business layer.

For further clarification, the above-mentioned phases are illustrated in a four-layer architecture of IoT in healthcare systems in Fig. 3. As shown in this figure, the vital signs of the user are obtained from wearable sensors. Then, obtained data are transferred to the smartphone via a connection like infrared. Eventually, the mobile device forwards this information to the database server (DB) through the network, such as the emerging 5G network. DB collects data from the sensors or the patient's announcement by pressing a button instantly. Other data are collected from health centers, including doctors' decisions and medical analytics, and are stored in the DB. Then, the system analyzes the stored data in the DB; afterward, the intelligent engine determines if normal data or abnormal data has taken place. When the system detects an abnormal situation, an alarm will be sent to the patient or doctor, and by approving the alarm, the patient will be hospitalized. Finally, with the increased demand to focus on recent advances in health systems and digital communications, patients can now connect to remote healthcare services anywhere, taking the highest sense of choice and customizing healthcare services.

2.3. Metrics definition

This section defines the metrics used to evaluate the proposed HIoT approaches, in brief as follows (Dhanvijay and Patil, 2019), (Asghari et al., 2018), (Bazzaz Abkenar et al., 2020a):

- *Security and privacy*: Security and privacy in smart healthcare systems are crucial, and some activities should be performed to protect health data against some attacks like side-channel attacks, physical attacks, malicious attacks, and preserve privacy, and prevent unauthorized access to health data (Cutillo et al., 2010).
- *Accuracy*: In healthcare systems, accuracy is very critical for caregivers. In IoT based healthcare systems, accuracy, based on the usage of the system, refers to the degree to which the captured data represents the real condition of the patient, the degree of captured data correctness and completeness, to the degree of computation correctness, and to what extent the taken decision is correct (Hogan and Wagner, 1997).
- *Performance*: Performance is serious for healthcare providers to collect accurate data, process the data, and provide services efficiently. This parameter is a mixture of network QoS parameters such as throughput, latency, delivery rate, mean time between failures, bandwidth usage, and other parameters like efficiency, load balancing, resource utilization, overhead, and computational time (as referred to in the reviewed papers) (Manishankar et al., 2017).
- *Time*: This parameter refers to how long it takes for users to receive service whenever requested. The concept of time includes execution time as run-time, computational time, average response time, and latency as the time delay in healthcare systems (Haghi Kashani et al., 2020a).
- *Cost*: It refers to the total cost that a healthcare service requester should pay to receive the best services. It includes the price of computation, communications, data storage, and maintaining the requested service (Bazzaz Abkenar et al., 2020a).
- *Energy*: Since the HIoT objects are resource-constrained and powered with limited energy resources, energy saving is vital to device and network survivability. Additionally, by growing the number of connected HIoT devices to the HIoT network, energy consumption in the HIoT network also increases. On the other hand, more energy consumption leads to an increase in operational costs and carbon production and decreases network lifetime (Jiang et al., 2020).
- *Interoperability*: Interoperability is the ability of two or more HIoT systems (for example, two or more medical informatics systems) to communicate, to exchange information accurately, consistently, and effectively, to use the information that has been exchanged, and to share resources between different systems (Dogac et al., 2007). Data interoperability is the ability to interpret data across systems or organizational boundaries correctly (Renner, 2001). In HIoT systems, it is mandatory to use standardized communication and some other technologies that support interoperability, like web services, clinical document architecture (CDA), and cloud computing.
- *Scalability*: It refers to the ability to extend and develop an IoT-based healthcare system when the number of service requests and demands increase. This ability can add smart devices, new operations as the service nodes for users', and network infrastructures without any reduction in the quality and performance of healthcare services. Expanding the system could be performed by adding new hardware or services to the system or by increasing the capability of the existing hardware or services (Chen et al., 2014).
- *Reliability*: The ability of a system to perform its required tasks in defined conditions and specified time. The aim of reliability in IoT-based healthcare systems is to deliver requested services successfully to the patients in most times and conditions (Bazzaz Abkenar et al., 2020a).

3. Related work and motivation

The related surveys and systematic reviews in HIoT systems are discussed in Section 3.1 to disclose the lack of comprehensive reviews and indicate the benefits and weaknesses of applied approaches systematically and taxonomically. Then based on a systematic search, the motivations in conducting this investigation are declared in Section 3.2.

3.1. Review studies on HIoT

The review studies based on surveys and SLRs are summarized in Table 1.

3.1.1. Surveys

Farahani et al. (Farahani et al., 2018) attempted to show an evolution from the clinic-based to the patient-based IoT healthcare systems. Furthermore, a holistic multi-layer IoT healthcare architecture was designed comprising devices, fog, and cloud layers to change traditional health systems to intelligent health systems. On the other hand, some important applications and services were described, such as mobile-health, anomaly detection, early warning score, ambient assisted living, as well as two case studies that were implemented, including intelligent eyeglasses for unobtrusive with constant heart rate monitoring with smart gloves in IoT for Parkinson disease. Additionally, challenges and barriers of this field were listed, such as data management, scalability, security, privacy, interoperability, and standardization. However, this review was not conducted systematically, and the process of articles selection, taxonomy, future works, and the covered years of the reviewed papers were not considered.

Darwish et al. (Darwish et al., 2017) introduced cloud computing and the IoT paradigm, called cloud IoT-health. In this survey, the authors explained the history of IoT and cloud computing and their applications in healthcare systems in detail, then incorporated them as a new technology to be used in healthcare systems. After that, some challenges and obstacles were defined in this scope, such as standardization, storage, scalability, and flexibility. Despite the appropriate explanations of this study, this review was not systematic, the paper selection process was not clear, no taxonomy of the selected papers was provided, and the covered years of the reviewed papers were unspecified.

Table 1
An overview of related surveys to HIoT.

Review type	Ref.	Main topic	Publication year	Paper selection process	Taxonomy	Open issue	Covered year
Surveys	Farahani et al. (2018)	Fog-driven IoT e-health	2017	Not clear	No	Not presented	Not mentioned
	Darwish et al. (2017)	IoT and cloud computing	2017	Not clear	No	Presented	Not mentioned
	Qi et al. (2017)	IoT for personalized healthcare	2017	Not clear	No	Presented	Not mentioned
	Qi et al. (2018)	Physical activity recognition and monitoring in IoT healthcare	2018	Not clear	No	Presented	2008–2018
	Dhanvijay and Patil (2019)	Technologies in IoT healthcare	2019	Not clear	Yes	Presented	Not mentioned
	Habibzadeh et al. (2020)	Healthcare IoT	2019	Not clear	No	Presented	Not mentioned
	Alam et al. (2018)	Communication technologies in Healthcare IoT	2019	Not clear	No	Presented	Not mentioned
	Ray et al. (2019b)	Edge computing in HIoT	2019	Not clear	Yes	Presented	Not mentioned
	Qadri et al. (2020)	Emerging technologies in the future of HIoT	2020	Not clear	Yes	Presented	Not mentioned
	Somasundaram and Thirugnanam (2020)	Security issues of HIoT	2020	Not clear	No	Not presented	Not mentioned
	Kadhim et al. (2020)	Patient's health monitoring system based on IoT	2020	Not clear	No	presented	Not mentioned
SLRs	Ahmed et al. (2018)	Security in IoT e-healthcare based on cloud	2018	Clear	Yes	Presented	2009–2017
	Ahmadi et al. (2018)	IoT in healthcare	2018	Clear	Yes	Presented	2000–2016
	Saheb and Izadi (2019)	Big data analytics and fog computing in HIoT	2019	Clear	Yes	Presented	2014–2018
	Usak et al. (2020)	IoT based healthcare service delivery	2020	Clear	Yes	Presented	2010–2018
	Zou et al. (2020)	User and data interaction in HIoT	2020	Clear	Yes	Presented	2018–2019
	Santos et al. (2020)	Heart monitoring system using IoT	2020	Clear	Yes	Presented	2015–2018
	Our study	IoT in healthcare	2021	Clear	Yes	Presented	2015–2020

Qi et al. (Qi et al., 2017) presented a study on advanced IoT that enabled personalized healthcare systems. In this investigation, a four-layer architecture including sensing, network, data processing, and application layers was designed, and all technologies used in these layers were explained in detail. Additionally, the authors discussed the challenges to motivate researchers for their future works. However, this survey was not systematic, and the paper selection process was not clear. Moreover, no taxonomy of the studied papers was provided, and the covered years of reviewed papers were not defined.

Qi et al. (Qi et al., 2018) illustrated a physical activity recognition and monitoring architecture in IoT layer-based perspective and expanded their scheme in four layers. In addition, future trends were described for researchers. However, contrary to the title of the article, this review was not conducted systematically. Also, there was not a unique selection process of studied articles or any classifications to give a clear vision to readers. Moreover, published papers in 2019 and 2020 were not considered. Also, Dhanvijay and Patil (2019) presented a survey that reviewed the latest important technologies and their applicabilities in IoT healthcare systems. Especially, they concentrated on WBAN and its security aspects. Moreover, there was a technology-based classification to give a clear vision to researchers. Also, some challenges have been addressed to extend this topic as future works. But, this investigation was not systematic, the process of selecting papers was not specific, and the covered years of papers were not mentioned.

Habibzadeh et al. (Habibzadeh et al., 2020) summarized the existing technologies in clinical practice healthcare, especially in three fields of sensing, communications, and analytics. Moreover, some important trends, challenges, and application demands were addressed. Afterward, the authors presented their supposed architecture, describing each layer, and trendy study directions as future works. Further, Alam, et al. (Alam et al., 2018) explored the key application-based requirements from the vision of communication-based technologies in HIoT. Also, some emerging technologies and standards used in this field were explained with different scenarios. Additionally, some future trends and challenges were highlighted for the future of HIoT. But, in these two surveys, investigations were not created systematically, the process of paper selection was not clear, and the taxonomy and covered years of studied papers were not specified.

Ray et al. (Ray et al., 2019b) reviewed the existing standards and solutions for the edge/IoT. Also, the authors suggested an architecture based on edge computing with its requirements, capabilities, functionalities, and operational issues. Then, there was a comparison between cloud computing and edge computing in HIoT in terms of latency and bandwidth utilization criteria to give an idea as future works for researchers. Furthermore, a taxonomy of industrial edge-IoT computing was defined. But, this paper was not systematic, the process of paper selection was not clear, and the covered years of this survey were not specified. Qadri et al. (Qadri et al., 2020) provided an overview of HIoT structure, and then, based on different use cases, various architectures were presented. Moreover, a large number of technologies that were appropriate for the future of HIoT, such as machine learning, blockchain, big data, edge computing, and software-defined network (SDN), were explored and analyzed. Also, two other technologies including the tactile Internet (TI) and Internet of nano things (IoNT) were suggested as future works. Furthermore, a taxonomy of emerging technologies, based on the quality of service (QoS), security and privacy, and diagnostic systems, was introduced. But, this review was not systematic, the method of paper selection was not distinctive, and the covered years of selected papers were not specified.

Somasundaram and Thirugnanam (2020) reviewed security issues, different risk factors of security attacks, and counter solutions related to the Internet of Medical Things (IoMT). The study showed that providing device-level security is necessary, and simultaneously, communication-level security has occurred on a moderate level. The experimental results showed that in IoMT, the DDoS attack and authentication issue in wireless insulin pump are harmful comparing with other security vulnerabilities with 95 % and 55 % risk factor, respectively. However, this review was not conducted systematically,

and the paper selection process with the taxonomy, future works, and the covered years of published papers was not considered. Kadhim et al. (Kadhim et al., 2020) reviewed the Internet-based healthcare monitoring systems, explored the uses of IoT applications in the medical sector, and how much it can enrich traditional medical methods, highlighting the extent of IoT ability of medical care services quality by having accurate diagnoses for patients. Moreover, the study helps to decreases periodic patient reviews to the hospital using IoT applications for remote diagnosis. However, they proposed a descriptive research approach, and this review was not conducted systematically, and the paper selection process with the taxonomy, future works, and the covered years of published papers were not considered.

3.1.2. SLRs

Ahmed et al. (Ahmed et al., 2018) reviewed the top existing security techniques and security threats used to systematically prevent malicious insider attacks and their applications in the HIoT and multi-cloud-based smart healthcare environment. Based on this survey, 60 % of all cyber-attacks were carried out by insiders. However, the published papers between 2018 and 2020 were not considered. Also, Ahmadi, et al. (Ahmadi et al., 2018) presented a systematic review of IoT in healthcare systems. In addition, the selected articles were categorized by a specified taxonomy comprising home health, m-health, e-health, and hospital management. Moreover, they described the application areas, applied technologies, and protocols in HIoT. Moreover, four communication models were introduced to explain how objects communicate with one another in different scenarios. Additionally, the distribution of articles by the publication year, application area, and journal or conference types were depicted. In the authors' view, standardization and interoperability were the main defects and limitations of the IoT in healthcare. However, the published papers between 2017 and 2020 were not addressed.

Saheb and Izadi (2019) presented a qualitative and quantitative systematic review on HIoT fog computing and big data analytics in detail. Additionally, they addressed some challenges as future directions for other researchers. However, published papers in 2019 and 2020 were not reviewed. Usak et al. (Usak et al., 2020) presented an SLR on the IoT-based health care service delivery, surveyed relevant articles, and provided a taxonomy of them, including the pharmaceutical industry, monitoring, and E-health categories. The selected papers were compared using some factors such as efficiency, energy savings, accuracy, speed, personal innovativeness, security, flexibility, quality, cost, and monitoring. The authors comparatively analyzed the advantages, drawbacks, and main challenges of current mechanisms, and produced results to develop much efficient IoT-based mechanisms in the future. The results showed that most of the papers aimed to improve remote monitoring, cost, and efficiency, whereas the security issue was less considered. However, the proposed SLR exclusively focused on service delivery issue while another studies exist over different related subjects such as economic, social, urban intelligence communities, which would be worth considering them by future studies. In addition, the published papers between 2019 and 2020 were not considered.

Zou et al. (Zou et al., 2020) reviewed the papers focused on people interacting with the HIoT data, highlighted various critical issues related to this concept, and discussed the data challenges which make difficult HIoT development. They categorized reviewed studies into three important HIoT data types and seven important HIoT end-user groups. However, the reviewed sample data and data extraction are somewhat inaccurate and published papers after 2018 were not considered. Also, Santos, et al. (Santos et al., 2020) analyzed the studies focused on online monitoring, detection, and support of the diagnosis of cardiovascular diseases. In addition, they studied how to address the security issues and provided a reference model to assist future developers in exploring the necessary factors to develop an online heart monitoring system prototype. Moreover, they presented an evaluating study to specify which electrocardiography (ECG) or photoplethysmography (PPG) technologies is the best to be developed. However, they just focused on cardiovascular diseases, and published papers from 2018 to 2020 were not considered.

3.1.3. Concluding remark

None of the previously SLRs (Ahmadi et al., 2018), (Saheb and Izadi, 2019), (Ahmed et al., 2018), (Usak et al., 2020), (Zou et al., 2020), (Santos et al., 2020) have investigated the IoT-based healthcare systems comprehensively. Saheb and Izadi (2019) studied big data in HIoT until 2018. Ahmed et al. (Ahmed et al., 2018) focused on the security issue in HIoT until 2017. Usak et al. (Usak et al., 2020) focused on service delivery in HIoT and the covered years were between 2010 and 2018. Zou et al. (Zou et al., 2020) investigated user and data interaction in HIoT, and they reviewed the studies between 2018 and 2019 that seem to be insufficient. Santos et al. (Santos et al., 2020) reviewed papers related to heart monitoring systems using IoT environment. However, the covered years were between 2015 and 2018. Ahmadi et al. (Ahmadi et al., 2018) is the closest work to ours; however, the covered years were until 2016. In consequence, we believe that our SLR is the first attempt to explore HIoT systems comprehensively until 2020.

3.2. The motivations for a secondary study on HIoT

The motivation of conducting an SLR is *identification, classification,* and *evaluation* of the existing approaches in HIoT. It mainly puts emphasis on classification and comparison of the existing methods in this field. To show that no comprehensive SLR has been reported until 2020, we searched Google Scholar with the following search string:

(healthcare <OR> health <OR> e-Health).
[AND]
("Internet of Things" <OR> IoT).
[AND]
(survey <OR> review <OR> overview <OR> study <OR> challenges <OR> "state of the art" <OR> trends).

Most of the studied review papers up to 2020 did not provide any analytical and taxonomic classifications to shed light on the open challenges. A summary of the studied reviews is presented in Table 1, which shows the reviews' parameters, including review type, main topic, publication year, paper selection process, taxonomy, open issue, and covered year for each study. It is observed that only one paper (Ahmadi et al., 2018) has applied the SLR method to study IoT in healthcare explicitly between 2000 and 2016, and the others used the SLR method to review security, big data, service delivery, data interaction, and heart monitoring in HIoT; additionally, they have covered fewer years (See Section 3.1.3). Therefore, our study is the first paper that has used an SLR method to explore IoT in healthcare systems until 2020. Due to the cases mentioned above, a comprehensive investigation has been carried out to cover the following disadvantages:

- The organization of some reviews was not systematic in HIoT, and the paper selection process was not clear.
- Some surveys reviewed the selected papers without providing any analytical classifications in HIoT.
- Open issues in HIoT were not discussed in some of the reviews.
- Most of the published articles, especially in 2019 and 2020, were not considered.
- Some articles had not studied evaluation metrics in HIoT.
- Some other articles had not mentioned the evaluation tools.

4. Research method

Contrary to an unstructured review process, the SLR method was applied to reduce bias and to follow a rigorous and precise sequence of methodological phases to research literature. An SLR depends on the well-defined review protocol to extract, evaluate, and document results (KitchenhamKeele, 2004; Jamshidi et al., 2013; Haghi Kashani et al.,

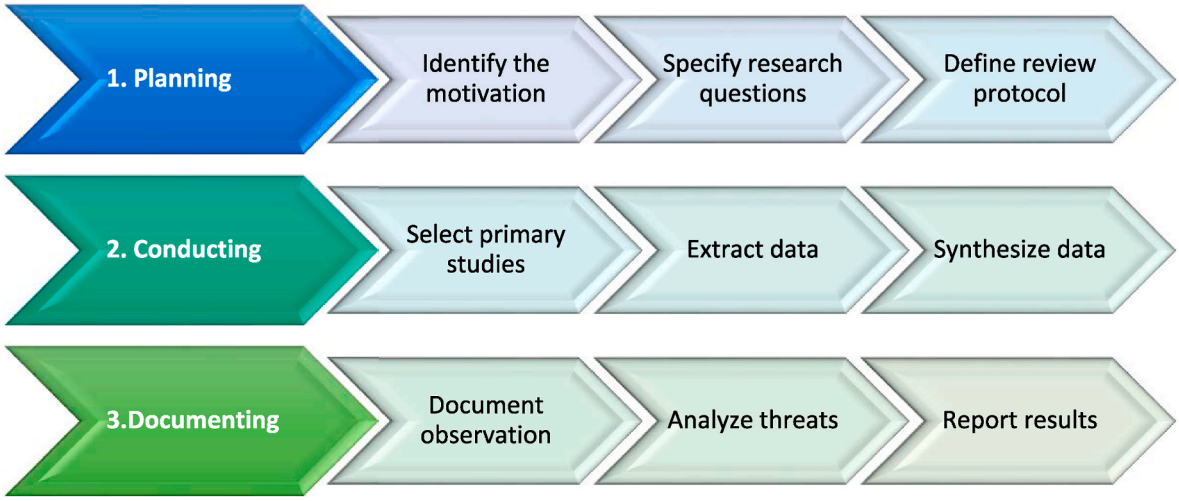

Fig. 4. An overview of our research methodology.

2020b; Songhorabadi et al., 2020; Bazzaz Abkenar et al., 2020b), as depicted in Fig. 4. Then, an SLR method that includes *planning, conducting, and documenting* is applied. The review is completed by an external evaluation for the consequences of each phase. A summary of the planning and conducting phases used to perform this SLR is presented in this section. Afterward, the results are reported in terms of data summary in Section 6 and research implications and findings in Section 7.

4.1. Planning the systematic review

Planning begins with the identification of the motivations for an SLR method and results in a review protocol as follows:

Stage 1. Identifying the motivations for the systematic review: The motivation is addressed and the contribution of this systematic review is described in Section 3.2.

Stage 2. Defining the research questions: The RQs that are based on our motivations and responses provide an evidence-based overview of HIoT systems. In this regard, four research questions that present the basis of deriving the search method for selecting articles are specified. The main objective of the research for each question is provided by the motivations that are shown in Table 2. Further, a comparative analysis that helps us to consider the importance of this research is presented as an analysis of the results in Section 6.

Stage 3. Defining and evaluating the review protocol: Up to this point, we specified the RQs and the study scope to adjust search terms for research extraction. In addition, a review protocol to achieve a systematic study was applied based on our experience with SLRs (Haghi Kashani et al., 2020a), (Asghari et al., 2019a), (Asghari et al., 2018), (Bazzaz Abkenar et al., 2020a), (Rahimi et al., 2020), (Bazzaz Abkenar et al., 2020a), (Ahmadi et al., 2021). A pilot study of the SLR, with 20 percent of our studies, is conducted to evaluate this method. Reducing the bias among researchers is the principal aim of this pilot study. Therefore, the search strategies, review scope, and refined inclusion/exclusion criteria are improved.

Table 2
Research questions and the motivations.

Research Questions	Rationales
RQ1: What are the major practical motivations behind associating IoT in healthcare systems?	The purpose is to gain insight into what are the primary reasons for applying IoT in healthcare systems.
RQ2: What research scopes do exist in IoT-based healthcare systems? Besides, what achievements are there in this area?	The purpose is to have a perception of what research scopes are available in HIoT and what are the merits and demerits of each.
RQ3: What are the existing techniques and methods to enable IoT in healthcare systems?	The purpose is to identify and compare existing factors, techniques, and tools that support HIoT.
RQ4: What are the key open issues, future trends, and challenges in IoT-based healthcare systems?	The purpose is to reveal the research opportunities and future directions in this field.

Table 3
Research criteria.

Criteria	
Inclusion	1. Research articles that present solutions, experiences, or evaluation of HIoT 2. Research articles from 2015 to 2020 3. JCR-indexed journal articles
Exclusion	1. Research articles that do not explicitly discuss HIoT 2. Books, book chapters, conference papers, symposiums, and non-English scripts 3. Commentaries or review articles 4. Short articles (less than six papers)

4.2. Conducting the systematic review

The conducting phase includes article selection, the outcome in extracted data, and information synthesizing.

Stage 1. Selecting primary articles: In this step, we explored the search string of.

(healthcare <OR> *health* <OR> *e-Health)* [AND] *(IoT* <OR> *"Internet of Things")*

through Google Scholar as the main search engine based on popular academic publishers such as ACM, Emerald, Hindawi, IEEE, Inderscience, SAGE, Science Direct, Springer, Taylor and Francis, and Wiley. Additionally, the paper selection process is illustrated in Fig. 5, as follows:

- *Initial selection*: This step includes filtering the titles, abstracts, and keywords of potential primary articles. This stage resulted from 1343 articles, including conference papers, journals, chapters, books, symposiums, and other types of literature that were part of this search term. The search string was applied to address digital databases from 2015 to 2020.
- *Final selection*: Table 3 shows the inclusion/exclusion criteria used to include relevant articles and exclude irrelevant ones. Due to the wide range of literature on HIoT systems and despite the acquired reputed conference articles, only journal citation reports (JCR)-indexed articles were considered. Moreover, full-text evaluation and analysis of

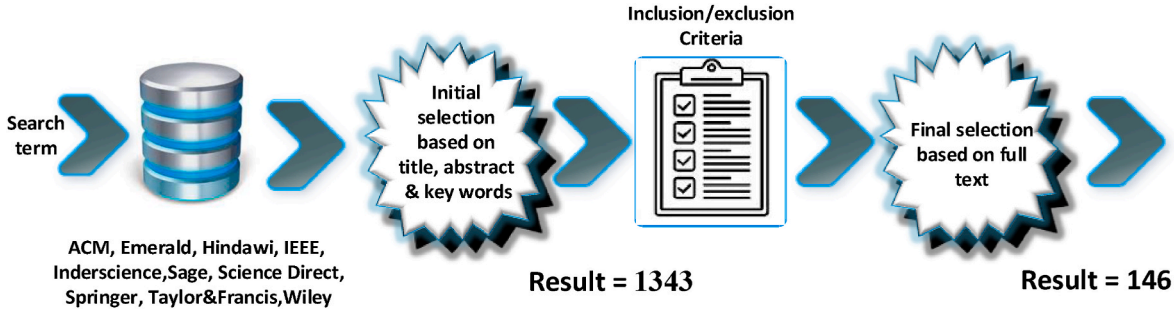

Fig. 5. Primary study selection process.

the JCRs were performed in the final selection stage to select related journals about HIoT. We retrieved 146 related JCR-indexed journal articles.

Stage 2 and 3. Data extraction and synthesis: We obtained data from a list of mentioned online search databases and designed a structural format based on aspects of characterization, using the guidelines provided by (Brereton et al., 2007), (KitchenhamKeele, 2004). We compared the proposed approaches for HIoT in Section 5, analyzed the advantages and disadvantages of the existing researches in Section 6, and presented future trends in Section 7.

5. Taxonomy for IoT-based healthcare systems

In this section, 146 retrieved journal articles are discussed. Furthermore, their main idea, evaluation techniques, tools, advantages, and disadvantages are explained. Since the literature on HIoT is widely diverse, systematic arranging of relevant studies is difficult. According to the studies on relevant investigations as researchers' challenges, our classification was natural. Based on the efforts made to review papers, some of them were found to be under the same umbrella covering the sensor-based approaches, and the remainders were resource-based, communication-based, application-based, and security-based perspectives. Therefore, the presented approaches in this review have been classified into five main distinct categories shown in Fig. 6, while other classifications could be possible. All approaches have been reviewed and summarized in Sections 5.1, 5.2, 5.3, 5.4, and 5.5.

5.1. Sensor-based approaches

Reviewing the articles showed that some of the literature emphasized the sensors and medical devices in HIoT and could be divided into two categories, including wearable sensors and environmental sensors. The selected sensor-based articles are reviewed in Section 5.1.1. A summary of the retrieved information from studied papers and a comparison between them are discussed in Section 5.1.2.

5.1.1. An overview of the selected sensor-based approaches

In this section, we study sensor-based articles, including wearable sensors and environmental sensors.

5.1.1.1. Wearable sensors. This subsection reviews the articles related to wearable sensor including (Ray et al., 2019c), (Bhatia and Sood, 2017), (Azimi et al., 2019), (Yang et al., 2016), (Wu et al., 2017), (Wu et al., 2018), (Niitsuet al., 2018), (Tekeste et al., 2019), (Hallforset al., 2018), (Esmaeili et al., 2020), (Muthuet al., 2020), (Huifeng et al., 2020), (Wu et al., 2020).

Ray et al. (Ray et al., 2019c) proposed wearable and cost-effective galvanic skin response (GSR) system to detect an individual's level of human physiological activities by amplifying, acquiring, and processing GSR data in smart e-healthcare applications. In addition, the obtained data were shown in users' smartphones with low power consumption. However, security and privacy requirements were ignored. Bhatia and Sood (2017) illustrated an intelligent healthcare framework to provide ubiquitous healthcare during people's workout sessions by analyzing real-time health conditions obtained from gyms through people's wristband, and to predict health state vulnerabilities using an artificial neural network (ANN). The results of experiments showed that the proposed system has high performance and efficiency. Azimi et al. (Azimi et al., 2019) presented personalized missing data resilient decision-making method to deliver health decisions. They used a case study on pregnant women to monitor their maternal health via their wristband and proved that their model was more accurate when the missing window was large. However, security and privacy issues were ignored. Further, Yang, et al. (Yang et al., 2016) presented a portable and wearable system for long-term electrocardiogram (ECG) signal detection system with low cost, high accuracy, and reliability. The experimental results showed suitable system accuracy and reliability. The main defect of these two papers is lack of security and privacy issues to satisfy the security requirements of the system.

In another research, Wu, et al. (Wu et al., 2017) offered a wearable sensor-based system with solar energy harvesting to extend the lifetime of sensor nodes and the Bluetooth low power transmission. This system enabled the implementation of an autonomous WBAN for IoT to measure the body's temperature distribution and heartbeat to detect falls. However, this study lacked security and privacy requirements. Wu et al. (Wu et al., 2018) presented a wireless implantable sensor prototype with flexible subcutaneous solar energy harvesting as a self-powered system that was able to restart in battery discharge conditions. Although the prototype incorporated Bluetooth low energy module and temperature sensor, the security was ignored.

Niitsu et al. (Niitsuet al., 2018) suggested a self-powered disposable supply-sensing biosensor platform using an organic biofuel cell for big data-based healthcare applications in IoT, which was environmentally friendly and had high performance. Tekeste et al. (Tekeste et al., 2019) introduced a real-time QRS (Q, R, and S are waves on an ECG line) detector and an ECG compression architecture for energy consumption for IoT healthcare wearable devices. Moreover, the experimental results showed high sensitivity and predictivity of the suggested architecture. However, security and privacy were ignored. Hallfors et al. (Hallforset al., 2018), on the other hand, introduced the characterization, fabrication, and validation of composite fabric ECG self-powered wearable IoT-based sensors that were made of nylon with reduced graphene oxide (rGOx). Based on the experimental results, the rGOx showed high performance in terms of noise level for ECG signal amplitudes.

Further, Esmaeili, et al. (Esmaeili et al., 2020) proposed a secure lightweight sensing scheme for body area networks that labels patients' data based on a priority mechanism and offers the services to emergency patients with low delay. Muthu et al. (Muthuet al., 2020) designed IoT-connected wearable sensors empowered with artificial intelligence (AI) and machine learning, which predict diseases, inform patients, and

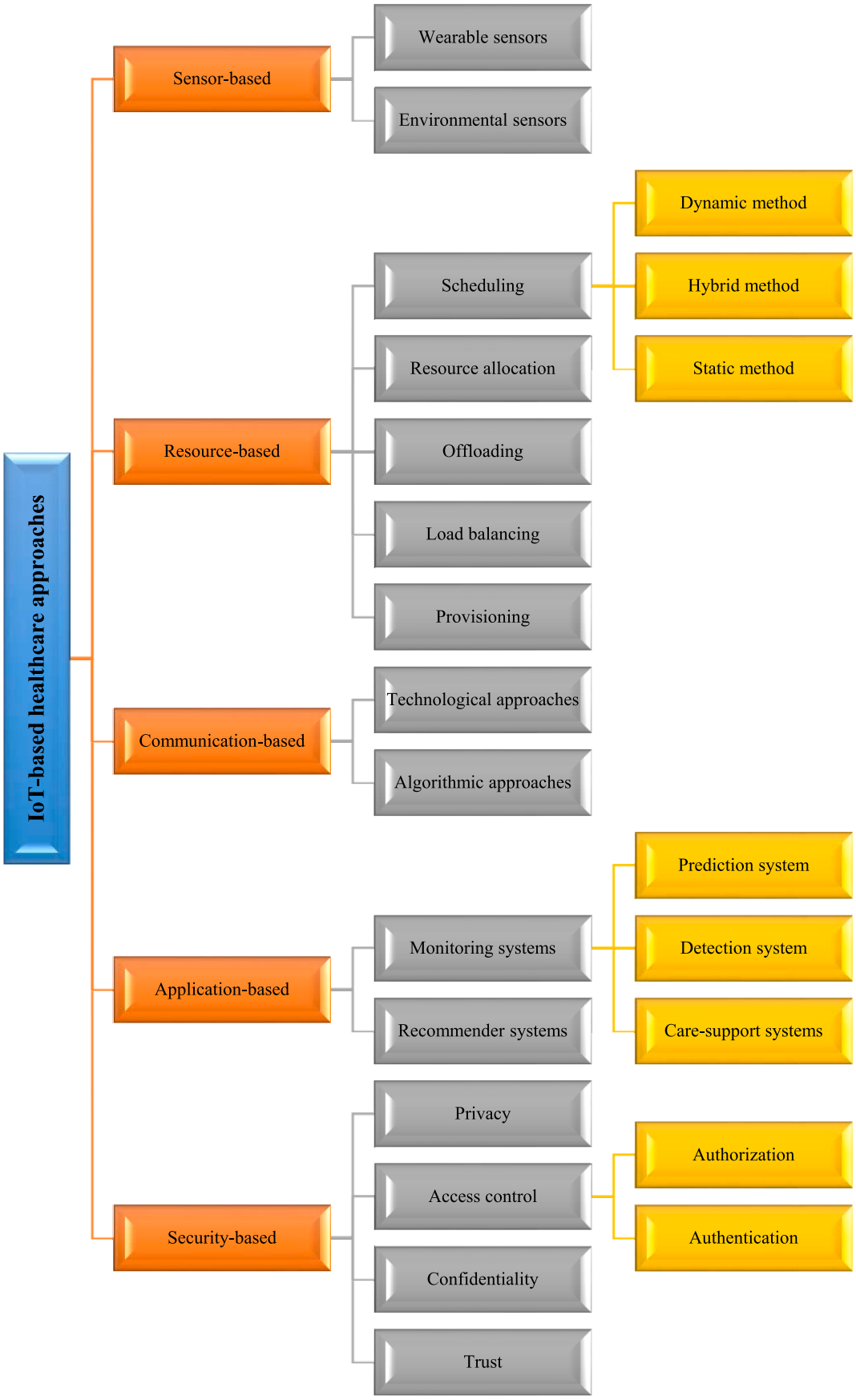

Fig. 6. A taxonomy of the selected articles in IoT-based healthcare.

provide treatments. Huifeng et al. (Huifeng et al., 2020) presented IoT-based wearable sensors and machine learning that continually collects the health parameters and traces the exercises to monitor the sport person's health condition. Wu et al. (Wu et al., 2020) designed a compact wearable sensor patch to measure various physiological parameters such as ECG, PPG, and body temperature that facilitates remote health monitoring providing security and privacy.

5.1.1.2. Environmental sensors. The articles related to environmental sensors, including (Vilela et al., 2019), (Ray et al., 2019d), (Elstset al., 2018), and (Chen et al., 2018), are reviewed as follows:

Vilela et al. (Vilela et al., 2019) introduced a fog-assisted health monitoring system for real-time applications and used it in the hospital as a scenario to prove its high performance and security. However, the interoperability among heterogonous devices was a big challenge in this study. Ray et al. (Ray et al., 2019d) prototyped a non-invasive, low power, and cost-effective sensor system to monitor real-time intravenous (IV) fluid bag level in e-healthcare applications. By using this

Table 4
The selected sensor-based approaches and their information.

Scope	Article	Main idea	Evaluation technique(s)	Tool(s) and evaluation environment(s)	Advantage(s)	Disadvantage(s)
Wearable sensors	Ray et al. (2019c)	A galvanic skin response system in smart e-healthcare applications	Prototype	Android	➢ High performance ➢Low energy ➢Low cost	➢Low security ➢Low scalability
	Bhatia and Sood (2017)	An intelligent real-time healthcare framework to predict the health state of the person during the workout	Real testbed	Not mentioned	➢High performance ➢High efficiency ➢High security ➢High stability	➢Low scalability
	Azimi et al. (2019)	A personalized approach for maternal health	Real testbed	Python	➢High accuracy ➢High reliability	➢Low security ➢Low scalability
	Yang et al. (2016)	An ECG-based monitoring system in HIoT	Real testbed	Not mentioned	➢High reliability ➢High accuracy ➢Low cost	➢Low security ➢Low scalability
	Wu et al. (2017)	A wearable sensor node with solar energy harvesting in HIoT	Simulation	LTspice	➢High reliability ➢High flexibility ➢Low energy	➢Low security ➢Low scalability ➢Low stability
	Wu et al. (2018)	A wireless implantable sensor for IoT healthcare applications	Simulation	Not mentioned	➢High flexibility ➢high performance ➢Low energy	➢Low security ➢Low privacy ➢Low scalability
	Niitsuet al. (2018)	A self-powered and disposable supply-sensing biosensor platform for big data in healthcare IoT	Simulation	SPICE	➢High performance ➢Low cost ➢Low energy	➢Low security ➢Low privacy
	Tekeste et al. (2019)	A real-time QRS detector to save energy consumption	Real testbed	Verilog-RTL	➢High performance ➢High efficiency ➢High optimization ➢High reliability ➢Low energy	➢Low security
	Hallforset al. (2018)	Nylon ECG wearable sensors in HIoT	Simulation	SPICE	➢High efficiency ➢Low energy	➢Low security ➢Low scalability
	Esmaeili et al. (2020)	A secure sensing scheme for body area networks in HIoT	Simulation	MATLAB	➢High security ➢Low energy ➢Low packet delivery delay	➢Low interoperability ➢Low scalability
	Muthuet al. (2020)	A wearable sensor empowered with AI and machine learning	Simulation	MATLAB	➢High sensitivity ➢High specificity ➢High accuracy ➢High precision ➢High performance	➢Low security ➢Low privacy
	Huifeng et al. (2020)	Sportsperson health monitoring system using wearable sensor	Simulation	MATLAB	➢High accuracy ➢Low error rate ➢High precision ➢High F-score ➢High performance	➢Low security ➢Low privacy
	Wu et al. (2020)	A wearable sensor patch to measure health parameters in HIoT	Real testbed, Prototype	Not mentioned	➢High security ➢High privacy ➢High performance	➢Low scalability
Environmental sensors	Vilela et al. (2019)	A fog-assisted health monitoring system	Prototype	Not mentioned	➢High security ➢High performance ➢Low energy	➢Low interoperability ➢Low scalability
	Ray et al. (2019d)	A sensor-based system to monitor the real-time intravenous fluid bag level in e-healthcare applications	Prototype	Not mentioned	➢High performance ➢Low latency ➢Low energy ➢Low cost	➢Low security ➢Low scalability
	Elstset al. (2018)	SPHERE HIoT-based platform in smart homes	Real testbed	Contiki	➢High interoperability ➢Low cost ➢Low energy	➢Low scalability
	Chen et al. (2018)	An optimal packet size selection and power management for WSN in HIoT	Simulation	MATLAB	➢High performance ➢High reliability ➢Low latency ➢Low energy	➢Low security ➢Low scalability

application, caregivers could monitor the IV fluid bag's status on the web page to see whether it was about to get empty.

Moreover, Elsts, et al. (Elstset al., 2018) suggested a multi-modal platform called SPHERE and used it in smart home application to reduce power consumption and cost to monitor people in residential environments. The authors explained that the network architecture embraced software and hardware requirements in SPHERE. Finally, Chen, et al. (Chen et al., 2018) proposed three algorithms to improve packet size and power management selection in e-health WSNs. These three algorithms were compared with one another in terms of performance, latency, reliability, and lifetime.

5.1.2. A summary of sensor-based approaches

Sensor-based approaches focus on the aspects of medical devices and sensors in two categories, including wearable sensors and environmental sensors that are responsible for measuring vital signs of patients' bodies. The proposed approaches along with their main ideas, evaluation techniques, tools, benefits, and weaknesses, are explored in Table 4. Moreover, a comparison of proposed approaches in terms of security, accuracy, performance, reliability, time, cost, and energy is shown in Table 5.

5.2. Resource-based approaches

Due to the resource heterogeneity, resource limitations, dynamic nature, and unpredictability of the HIoT environment, it is crucial to consider resource management issues as one of the challenging problems. In Section 5.2.1, some resource-based articles that focused on scheduling, resource allocation, offloading, load balancing, and provisioning are studied. Afterward, in Section 5.2.2 the evaluation techniques and positive and negative points of the studied articles are presented.

5.2.1. An overview of the selected resource-based approaches

Reviewing the selected resource-based articles showed that they could be divided into five subcategories, including scheduling, resource allocation, offloading, load balancing, and provisioning.

5.2.1.1. Scheduling. Scheduling approaches, including three types of dynamic methods (Ray et al., 2019a), (Abdelmoneem et al., 2020), hybrid method (Yi and Cai, 2019), and static methods (Awanet al., 2019), (Manikandan et al., 2020), are explained in this subsection.

Ray et al. (Ray et al., 2019a) investigated three possible solutions where IoT could benefit from the real-time effects. Moreover, the authors presented a context-aware dew computing-based architecture for time-critical scenarios along with a delay-tolerant architecture for dynamic scheduling different tasks on resources. Abdelmoneem et al. (Abdelmoneem et al., 2020) proposed heuristic-based mobility-aware scheduling and allocation method that dynamically distributes tasks of healthcare systems on fog or cloud computational nodes based on patient movement, thereby provides load balancing. In addition, Yi and Cai (2019) proposed a scheduling management model to decrease the delay of medical packet transmission in HIoT systems. This model prevented gateways from misreporting the priority level of medical packets. Awan et al. (Awanet al., 2019) designed a priority-based congestion-avoidance routing protocol to enhance energy efficiency in multi-hop WBANs in HIoT systems. Additionally, the high performance of this protocol was proved in terms of stability, traffic load, lifetime, delay, throughput, optimization, and energy consumption. However, the mobility of sensor nodes was ignored in these studies, and the lack of security aspects seems to be the main shortcoming of them. Manikandan et al. (Manikandan et al., 2020) proposed a hash-based polynomial method that classifies the patients' data based on their health condition (normal or critical) and then efficiently schedules them to be processed.

5.2.1.2. Resource allocation. The articles focused on resource allocation including (Asif-Ur-Rahmanet al., 2019), (Kavitha and Sharma, 2019), (Sengupta and Bhunia, 2020), and (Awaisi et al., 2020), are reviewed as follows:

Asif-Ur-Rahman et al. (Asif-Ur-Rahmanet al., 2019) offered a real-time heterogeneous HIoT framework along with employing SDN and link adaptation. Additionally, this framework focused on optimal and efficient resource utilization and resource allocation. Simulation proved that this framework has high QoS, low packet loss, and end-to-end latency. However, the framework suffers from high complexity and a lack of security. Kavitha and Sharma (2019) replaced the default first-come-first-serve virtual machine allocation scheme with an ant colony optimization (ACO) scheme to show how ACO could optimally utilize resources in the cloud and decrease response time in life-critical healthcare applications. However, the security and scalability of the scheme were not considered. Sengupta and Bhunia (2020), using cloudlet and IoT, proposed a data management scheme that facilitates real-time store and retrieval of enormous e-Health data, thereby improves energy consumption, response time, and packet loss. Awaisi et al. (Awaisi et al., 2020) used the virtual machine partitioning concept in fog nodes to propose an efficient architecture based on fog for healthcare systems and exploited elliptic curve cryptography for user authentication.

5.2.1.3. Offloading, load balancing, and provisioning. Other resource-

Table 5
A comparison of the evaluation factors in the sensor-based approaches.

Scope	Article	Security	Accuracy	Performance	Reliability	Time	Cost	Energy
Wearable sensors	Ray et al. (2019c)			*			*	*
	Bhatia and Sood (2017)	*		*	*			
	Azimi et al. (2019)		*		*			
	Yang et al. (2016)		*		*		*	
	Wu et al. (2017)				*			*
	Wu et al. (2018)			*				*
	Niitsuet al. (2018)			*			*	*
	Tekeste et al. (2019)			*	*			*
	Hallforset al. (2018)			*				*
	Esmaeili et al. (2020)	*				*		*
	Muthuet al. (2020)		*	*				
	Huifeng et al. (2020)		*	*				
	Wu et al. (2020)	*		*				
Environmental sensors	Vilela et al. (2019)	*		*				*
	Ray et al. (2019d)			*		*	*	*
	Elstset al. (2018)						*	*
	Chen et al. (2018)			*	*	*		*

based approaches, including offloading (Minet al., 2019), (Wang and Li, 2020), (Wang and Cai, 2020), load balancing (He et al., 2017), (Bharathiet al., 2020), and provisioning (Kumar and Silambarasan, 2019), are described in this subsection.

Min et al. (Minet al., 2019) presented a privacy-aware scheme to help IoT healthcare devices to protect their privacy, using the reinforcement-learning method. Indeed, this scheme helps HIoT devices select the offloading rate, improves computation performance, reduces latency, protects users' privacy, and saves devices' energy. Wang and Li (2020) leveraged fog computing capabilities in terms of in-network caching and request aggregation to reduce the latency of patient data retrieval; thereby, the latency was reduced by nearly 28.5 %. Wang and

Table 6
The selected resource-based approaches and their information.

Scope	Article	Main idea	Evaluation technique(s)	Tool(s) and evaluation environment(s)	Advantage(s)	Disadvantage(s)
Scheduling	Ray et al. (2019a)	A real-time HIoT-based resource scheduling framework	Simulation	PubNub, Raspberry Pi3, Arduino Mega2560	➢High optimization ➢Low latency	➢Low security ➢Low privacy
	Abdelmoneem et al. (2020)	A dynamic heuristic-based mobility-aware task scheduling and resource allocation framework	Simulation, Real testbed	iFogSim	➢Low makespan ➢Low network load ➢Low energy ➢Low latency	➢Low scalability ➢Low fault-tolerant ➢Low security
	Yi and Cai (2019)	Scheduling management of WBAN packet transmission scheme	Simulation	Not mentioned	➢High reliability ➢High performance	➢Low security ➢Low privacy
	Awanet al. (2019)	A multi-hop priority-based congestion-avoidance routing protocol using IoT-based sensors in WBANs	Simulation	MATLAB	➢High stability ➢High performance ➢Low energy	➢Low security ➢Low privacy ➢Low mobility
	Manikandan et al. (2020)	Smart healthcare scheduling using IoT and decision tree	Simulation	Not mentioned	➢Low scheduling time ➢High accuracy ➢High efficiency ➢Low overhead ➢High performance	➢High power consumption ➢High cost ➢Low scalability
Resource allocation	Asif-Ur-Rahmanet al. (2019)	A heterogeneous cloud-based framework in HIoT	Simulation	Not mentioned	➢High optimization ➢Low latency	➢Low security ➢Low privacy
	Kavitha and Sharma (2019)	Analyzing the performance of ACO-based VM allocation in the cloud for HIOT	Simulation	CloudSim	➢High performance ➢High stability ➢Low latency	➢Low scalability ➢Low security ➢Low privacy
	Sengupta and Bhunia (2020)	Using cloudlet and IoT to improve e-Health data store and retrieval	Simulation	Not mentioned	➢Low energy ➢Low response time ➢Low packet loss	➢High computation overhead ➢High communication cost ➢Cloudlet failure
	Awaisi et al. (2020)	Using VM partitioning concept in fog nodes for HIoT architecture	Simulation	iFogSim	➢Low latency ➢Low network usage ➢High privacy ➢High performance	➢Low scalability
Offloading	Minet al. (2019)	A reinforcement learning-based privacy-aware offloading scheme in HIoT	Simulation	Not mentioned	➢High privacy ➢Low latency ➢Low energy	➢Low security ➢Low scalability
	Wang and Li (2020)	Using fog in-network caching to reduce the latency of patient data retrieval	Simulation	NS-3	➢Low latency	➢Low security ➢Low privacy
	Wang and Cai (2020)	Using IoT, NDN, and edge cloud to reduce the latency of patient data retrieval	Simulation	NS-3	➢Low latency ➢Low communication cost	➢Low reliability
Load balancing	He et al. (2017)	A proactive personalized service through fog and cloud Computing framework	Prototype	Ubuntu 16.04	➢High optimization ➢High scalability ➢Low latency	➢Low security ➢Low privacy
	Bharathiet al. (2020)	An energy-efficient sensor clustering technique using particle swarm optimization	Simulation	Not mentioned	➢High sensitivity ➢High specificity ➢High accuracy ➢High f-score ➢Low energy	➢Low performance
Provisioning	Kumar and Silambarasan (2019)	Using optimized techniques to increase the performance of cloud in HIoT systems	Simulation	MATLAB, CloudSim	➢High efficiency ➢Low latency	➢Low security ➢Low privacy

Cai (2020) combined IoT, Name Data Networking (NDN), and edge cloud to design a secure and efficient data management scheme that improves medical data storage and retrieval.

Further, He, et al. (He et al., 2017) proposed a proactive hierarchical fog-cloud computing for complex event processing architecture to deal with the complexity of personalized services in large-scale applications. To this end, the graph partitioning theory was used to design load balancing algorithm of fog computing. Additionally, efficiency, real-time detection, low latency, and redundancy were validated in this scheme. Bharathi et al. (Bharathiet al., 2020) presented an energy-efficient sensor clustering technique to effectively select cluster heads. They tried to optimize parameters such as sensitivity, specificity, accuracy, F-score, and energy consumption. Finally, three resource optimization methods for virtual machines (VMs) in the cloud system, including the Cuckoo search method, artificial bee colony (ABC), and particle swarm optimization, were introduced by Kumar and Silambarasan (2019) to schedule resources. Simulation results showed that the ABC was more efficient than the other two techniques.

5.2.2. A summary of resource-based approaches

Resource-based approaches focus on resource management issues. These approaches include five subcategories: scheduling, resource allocation, offloading, load balancing, and provisioning. The resource-based articles along with main ideas, assessment techniques, tools, merits, and demerits, are shown in Table 6. In addition, a comparison of some metrics like optimization, performance, reliability, time, and energy, is shown in Table 7.

5.3. Communication-based approaches

The next group of classification refers to the communication-based methods. This section addresses communication infrastructures that are responsible for managing communications, including technological and algorithmic approaches. In Section 5.3.1, related articles and their communication technologies and algorithms are studied. Then, some obtained information about the given articles, such as evaluation techniques, benefits, and limitations, is presented in Section 5.3.2.

5.3.1. An overview of the selected communication-based approaches

The applied technological and algorithmic approaches between each of the nodes and layers of the HIoT network are reviewed in this subsection.

5.3.1.1. Technological approaches.

The articles related to technological approaches, including (Catarinucciet al., 2015), (Catherwood et al., 2018), (Abdellatif et al., 2018), (Aktas et al., 2018), (Chehri and Mouftah, 2020), and (Abuelkhail et al., 2020), are discussed as follows:

Catarinucci et al. (Catarinucciet al., 2015) introduced an IoT-based smart hospital system that uses different technologies, specifically smart mobile, RFID, and WSN, to guarantee automatic real-time tracking and monitoring of patients, staff, and biomedical devices within nursing institutes and hospitals for emergencies. Catherwood et al. (Catherwood et al., 2018) presented an advanced IoT-based analyzer and a LoRa/Bluetooth-enabled electronic reader for personalized monitoring with high coverage, portability, easy installation, and high battery lifetime. Abdellatif et al. (Abdellatif et al., 2018) designed an electroencephalogram (EEG) transceiver based on symbol-stream compression to achieve high performances in terms of data distortion, data reduction, low complexity, and energy consumption. Aktas et al. (Aktas et al., 2018) presented a HIoT framework associated with RFID and WBANs technologies for hospital information scenario that satisfied QoS requirements. Chehri and Mouftah (2020) proposed an impulse-radio ultra-wideband system to collect and analyze the patient's body vital signs with low complexity and energy consumption. Furthermore, Abuelkhail, et al. (Abuelkhail et al., 2020) built a network of smart nodes and clustered them periodically to reduce the load of RFID reader and decrease channel access congestion by receiving the data only from the cluster head instead of each individual node.

5.3.1.2. Algorithmic approaches.

The articles related to algorithmic approaches, including (Qiu et al., 2017), (Almobaideen et al., 2017), (Woo et al., 2018), (Ray et al., 2019e), (Chanak and Banerjee, 2020), (Sharavana Kumar and Sarma Dhulipala, 2020), and (Patan et al., 2020), are discussed in this subsection.

A self-recoverable time synchronization protocol for HIoT sensor networks that achieves high level of balanced energy consumption and accuracy was presented by Qiu et al. (Qiu et al., 2017). Almobaideen et al. (Almobaideen et al., 2017) designed a route selection approach based on the vicinity of medical centers besides selecting the shortest route for tourists with particular health conditions and the constant monitoring in emergencies. Woo et al. (Woo et al., 2018) presented a reliable M2M-based IoT system for personal healthcare devices with a fault-tolerant algorithm that employed backup copies, parity data, and daisy chain data. Moreover, the experiments showed the efficiency and high performance of the proposed system. Ray et al. (Ray et al., 2019e) presented two experiments to perform real-time visualization and

Table 7
A comparison of the evaluation factors in the resource-based approaches.

Scope	Article	Optimization	Performance	Reliability	Time	Energy
Scheduling	Ray et al. (2019a)	*			*	
	Abdelmoneem et al. (2020)				*	*
	Yi and Cai (2019)		*	*		
	Awanet al. (2019)		*	*		*
	Manikandan et al. (2020)		*		*	
Resource allocation	Asif-Ur-Rahmanet al. (2019)	*			*	
	Kavitha and Sharma (2019)		*	*	*	
	Sengupta and Bhunia (2020)				*	*
	Awaisi et al. (2020)		*		*	
Offloading	Minet al. (2019)				*	*
	Wang and Li (2020)				*	
	Wang and Cai (2020)				*	
Load balancing	He et al. (2017)	*			*	
	Bharathiet al. (2020)					*
Provisioning	Kumar and Silambarasan (2019)		*		*	

Table 8
The selected communication-based approaches and their information.

Scope	Article	Main idea	Evaluation technique(s)	Tool(s) and evaluation environment(s)	Advantage(s)	Disadvantage (s)
Technological approaches	Catarinucciet al. (2015)	A smart hospital system relies on different technologies	Prototype	Not mentioned	➢Low latency ➢Low energy	➢Low security ➢Low reliability ➢Low salability
	Catherwood et al. (2018)	An HIoT-based personalized wireless monitoring system	Simulation	Android	➢High accuracy ➢High reliability	➢Low sensitivity ➢Low security
	Abdellatif et al. (2018)	An EEG-based transceiver design for IoT healthcare	Simulation	Not mentioned	➢High performance ➢Low energy ➢Low overhead	➢Low security ➢Low privacy
	Aktas et al. (2018)	IoT healthcare system for biomedical applications	Simulation	Riverbed	➢High performance ➢Low latency ➢Low energy	➢High overhead ➢Low privacy
	Chehri and Mouftah (2020)	An impulse-radio ultra-wideband system for HIoT applications	Simulation	Not mentioned	➢High performance ➢High reliability ➢Low energy ➢Low overhead	➢Low security ➢Low reliability
	Abuelkhail et al. (2020)	RFID clustering scheme for IoT-based monitoring applications	Simulation, Prototype	MATLAB	➢High security ➢High data delivery ratio ➢Low transmission delay	➢Low scalability ➢Low QoS
Algorithmic approaches	Qiu et al. (2017)	A time synchronization protocol with self-recovery and high accuracy	Simulation	NS2	➢High accuracy ➢Low latency ➢Low energy	➢Low security ➢Low scalability
	Almobaideen et al. (2017)	A geographical routing for mobile tourists	Simulation	Not mentioned	➢High performance ➢Low latency	➢Low security ➢Low scalability
	Woo et al. (2018)	A fault-tolerant algorithm for the reliable HIoT systems	Real testbed	C#	➢High reliability ➢High performance ➢Low latency	➢Low security ➢Low scalability
	Ray et al. (2019e)	Real-time analytics at the edge of HIoT	Real testbed	Python, Arduino	➢Low latency ➢Low cost	➢Low scalability
	Chanak and Banerjee (2020)	Congestion free routing algorithm for healthcare applications	Simulation	NS-2	➢High throughput ➢High performance ➢Low energy consumption ➢High network lifetime ➢High received packet ratio	➢Low scalability
	Sharavana Kumar and Sarma Dhulipala (2020)	Fuzzy allocation model to assign data transfer time slots	Simulation	Not mentioned	➢Low average delivery delay ➢Low average energy consumption ➢High packet delivery ratio	➢Low security ➢Low safety
	Patan et al. (2020)	Improving QoS in IoT-based healthcare systems	Simulation	CloudSim	➢Low communication overhead ➢Low response time ➢High accuracy	➢Low security

Table 9
A comparison of the evaluation factors in the communication-based approaches.

Scope	Article	Accuracy	Performance	Reliability	Time	Cost	Energy
Technological approaches	Catarinucciet al. (2015)				*		*
	Catherwood et al. (2018)	*	*	*			
	Abdellatif et al. (2018)		*				*
	Aktas et al. (2018)		*		*		*
	Chehri and Mouftah (2020)		*	*			*
	Abuelkhail et al. (2020)			*	*		
Algorithmic approaches	Qiu et al. (2017)	*			*		*
	Almobaideen et al. (2017)		*		*		
	Woo et al. (2018)		*	*	*		
	Ray et al. (2019e)				*	*	
	Chanak and Banerjee (2020)		*	*			*
	Sharavana Kumar and Sarma Dhulipala (2020)			*	*		*
	Patan et al. (2020)				*	*	

analytics in a cost-effective and resource-constrained e-health sensor deployment scenario. The authors used several lightweight IoT protocol-based frameworks in their investigations. Chanak and Banerjee (2020) reduced routing congestion in healthcare applications by proposing a priority-based data routing strategy. The authors enhanced reliability by presenting a queue-based scheduling scheme. Sharavana Kumar and Sarma Dhulipala (Sharavana Kumar and Sarma Dhulipala, 2020) proposed a heuristic hybrid time slot fuzzy allocation algorithm that dynamically assigns time slots and improves packet delivery and packet distribution. Patan et al. (Patan et al., 2020) used a gray filter Bayesian convolutional neural network to reduce time overhead and improve data sensing and collection accuracy.

5.3.2. A summary of communication-based approaches

The communication technologies and algorithms applied in HIoT infrastructure are explained in this subsection. The communication-based articles along with their main ideas, positive and negative points, and other information, are detailed in Table 8. In addition, a comparison of evaluation factors such as accuracy, performance, reliability, time, cost, and energy is presented in Table 9.

5.4. Application-based approaches

In the next category, the application-based approach focuses on providing systems that can perform one or more specific services. In other words, an IoT-based healthcare system, beyond its sensor aspects, resource management, and communication infrastructure, produces the required services to patients, caregivers, or users. In this regard, the application-based category is divided into two sub-categories, including the monitoring systems and recommender systems. Moreover, the application-based articles are reviewed in Section 5.4.1, and the comparison of them is presented in Section 5.4.2.

5.4.1. An overview of the selected application-based approaches

This section provides an overview of the selected application-based approaches, including monitoring elderlies, recommending medicine and food, and other issues.

5.4.1.1. Monitoring systems. Reviewing the articles showed that the articles focused on patients monitoring included prediction systems (Verma and Sood, 2018), (Kumar et al., 2018), (Sood and Mahajan, 2019), (Verma et al., 2018), (Kaur et al., 2019), (Suresh et al., 2019), (Tan and Halim, 2019), (Rajan et al., 2020), (Satpathy et al., 2019), (Bhatia et al., 2020), (Vedaraj and Ezhumalai, 2020), (Fouad et al., 2020), (Akhbarifar et al., 2020), detection systems (Azimiet al., 2017), (Jebadurai and Dinesh Peter, 2018), (Khowaja et al., 2018), (Tuliet al., 2020), (Alam et al., 2019), (Alhussein et al., 2018), (Rajan et al., 2020), (Ray et al., 2018), (Hosseinzadehet al., 2020b), (Zgheib et al., 2020), (Rahmani et al., 2020), (AbdulGhaffar et al., 2020), (Kesavan and Arumugam, 2020), (Kavitha and Ravikumar, 2020), and care-support systems (Jabbar et al., 2017), (Rahmaniet al., 2018), (Laplante et al., 2018), (Ramírez López et al., 2019), (Onasanya and Elshakankiri, 2019), (Rajan Jeyaraj and Nadar, 2019), (Laplante et al., 2018), (Jeong and Shin, 2018), (Ghasemi et al., 2019), (Yanget al., 2018), (Onasanya et al., 2019), (Vedaeiet al., 2020), (Sharma et al., 2020), (Bandopadhaya et al., 2020).

Verma and Sood (2018) presented a cloud and IoT-based mobile--healthcare monitoring system for disease prediction. Additionally, the authors classified diseases into four subclasses and compared them in terms of accuracy, sensitivity, specificity, f-measure, and response time levels. Experimental results verified the security, stability, and practicability of the suggested system. Kumar et al. (Kumar et al., 2018) proposed a cloud/IoT-based mobile healthcare application to monitor, diagnose, and predict serious diseases. Additionally, they suggested a classification algorithm (fuzzy rule-based neural classifier) to decide on the medical dataset and diagnose the diabetes disease. Finally, the authors compared this algorithm with other existing models to validate it in terms of performance, security, and response time. However, this framework was vulnerable to some attacks related to advanced encryption standard (AES) and data encryption standard (DES) techniques.

Sood and Mahajan (2019) suggested a fog/IoT-based healthcare monitoring system to control hypertension disease. Additionally, ANN (artificial neural network) was applied to predict the risk level of hypertension, and the system was compared with cloud computing technology to prove its high bandwidth efficiency, low latency, and high accuracy in response time. Verma et al. (Verma et al., 2018) presented a smart monitoring student interactive healthcare system to predict specific diseases by utilizing data mining methods based on the k-cross validation method in computing waterborne symptoms. Based on the simulation, the suggested methodology performed better with low response time and high accuracy. Kaur et al. (Kaur et al., 2019) presented a framework based on a random forest machine-learning algorithm to monitor and predict diseases such as breast cancer, heart diseases, thyroid, diabetes, liver disorders, dermatology, and surgical data. Finally, the experimental results proved their accuracy; however, the security was ignored.

Suresh et al. (Suresh et al., 2019) proposed a real-time monitoring framework for HIoT systems. The authors integrated neural network classifiers and decision trees to report cancer progression with high prediction compared to other methods. Tan and Halim (2019) prototyped an embedded HIoT care monitoring system to measure body temperature, heart rate, and blood pressure. Additionally, the framework predicts diabetes and kidney disease in elderlies using the ANN classification model with high accuracy and low latency, compared with other conventional models. However, these two articles ignored the privacy and security of data transmission.

Rajan Jeyaraj and Nadar (Rajan et al., 2020) employed an intelligent electrocardiogram signal classification and a deep learning method to accurately predict and process many continuous-time series of ECG signals accurately in atrial fibrillation samples. Satpathy et al. (Satpathy et al., 2019) introduced a HIoT diagnosis system using a fuzzy classifier with a field-programmable gate array (FPGA) to predict the conditions of cardiovascular diseases with higher accuracy and lower latency. Furthermore, Bhatia, et al. (Bhatia et al., 2020) proposed a 4-layers system to monitor urine infection and predict Diabetes so that prudent steps can be taken at the early stages. Vedaraj and Ezhumalai (2020) presented a secure IoT-based architecture using Elliptical curve cryptography to predict heart and diabetic disease. Fouad et al. (Fouad et al., 2020) leveraged IoT sensors and AI to predict the exact health condition of the patient that helps to take the right assistance process. Akhbarifar et al. (Akhbarifar et al., 2020) presented a secure remote health monitoring model that uses a block encryption solution and data mining to predict the patient's health status and critical situation.

Azimi et al. (Azimiet al., 2017) proposed a hierarchical computing architecture called HiCH in HIoT monitoring systems to solve reliability and availability challenges in cloud-based architecture and limited computational resources in fog-based architectures. Besides, the architecture evaluation in terms of response time and bandwidth utilization on arrhythmia detection for the patients suffering from cardiovascular diseases (CVDs) shows its high performance compared to other existing models. However, energy consumption in the sensor network was not optimized.

Jebadurai and Dinesh Peter (Jebadurai and Dinesh Peter, 2018) presented hybrid architecture to process retinal images captured through smartphone in IoT healthcare systems. In addition, a learning-based single image super-resolution algorithm was used to improve the quality of the captured images for efficient detection. Khowaja et al. (Khowaja et al., 2018) proposed a fall and stress detection framework by applying some lightweight authentication protocols to collect the data securely based on contextual activity from wearable

sensors; however, the energy consumption issue was ignored.

Tuli et al. (Tuliet al., 2020) suggested a fog-based system in HIoT to detect heart diseases automatically using deep learning called healthfog. The authors validated their system to prove the real-time prediction, low power consumption, low latency, low bandwidth utilization, and high accuracy. However, the cost to implement this framework was ignored. An Internet of medical things-based emotion recognition system was proposed by Alam et al. (Alam et al., 2019). A deep convolutional neural network was applied to determine emotional states with high accuracy and performance through wearable biosensors that could complement context-aware recommendations, stress and depression management, and mood stabilization. Alhussein et al. (Alhussein et al., 2018) presented a cloud-based cognitive HIoT framework to detect seizure by using deep convolutional neural networks and the stacked autoencoder method. The framework is applicable in real-time emergencies with high accuracy and high sensitivity; however, security and privacy issues were ignored.

Rajan et al. (Rajan et al., 2020) presented an image pattern analysis along with an improved pixel distribution-based filter scheme in HIoT systems. A deep convolutional neural network was used to identify the oral cancer regions. The scheme increased accuracy and sensitivity in real-time scenarios, but security and privacy were ignored. Ray et al. (Ray et al., 2018) suggested an IoT-based mathematical model detect, monitor, and approximate fruit ripening quality index. Based on this research, 100 apples were selected to measure their ripening in a low-cost manner. In addition, there was a mathematical model for real-time fruit index measurement with cost-efficiency. This research was useful for the food industry and human health.

Hosseinzadeh et al. (Hosseinzadehet al., 2020b) used smart elderly care technologies to propose a health monitoring system based on IoT that continuously monitors the elderly's biological factors and behavioral activities. Zgheib et al. (Zgheib et al., 2020) used a semantic reasoning approach and proposed a framework to real-time monitor elderlies and detect their diseases. Rahmani et al. (Rahmani et al., 2020), using complex event processing, presented a three-layer event-driven architecture to analyze the data of IoT-based healthcare applications reliably. AbdulGhaffar et al. (AbdulGhaffar et al., 2020), using the Cisco packet tracer tool, proposed an IoT-based system to collect and process health data and offer medicine administration, diagnosis, and emergency services. Kesavan and Arumugam (2020), using a convolutional neural network, proposed a four-phase monitoring system that detects any abnormality situation and then notified or informs the doctor. Also, Kavitha and Ravikumar (2020) used neural networks and machine learning and designed an IoT-based monitoring system.

Jabbar et al. (Jabbar et al., 2017) simulated a resource description framework for heterogeneous IoT devices to provide semantic interoperability among physicians and patients with high performance as long-term support. Rahmani et al. (Rahmaniet al., 2018) introduced a fog computing-based architecture that could cope with some challenges in healthcare systems. In addition, they suggested smart geo-distributed gateways to end-users and sensors at the edge of the network to optimize the resources. Moreover, the healthcare monitoring system includes a suggested gateway applied in a medical case study to estimate the degree of illness in long-term caring. Laplante et al. (Laplante et al., 2018) presented an approach for three use cases (alcoholic, Alzheimer diseases, and patients' safety) as a long-term caring framework and discussed the related quality issues, particularly the need to consider caring as a requirement. Ramírez López et al. (Ramírez López et al., 2019) proposed a monitoring system for respiratory disorders to increase oxygen saturation and decrease energy consumption; this study was validated in terms of security and privacy issues. Onasanya and Elshakankiri (2019) suggested business analytics/cloud services and cancer care based on WSN/IoT technology to improve the existing treatment solutions. The system was compared to other similar systems to prove appropriate security, reliability, and scalability. Rajan Jeyaraj and Nadar (Rajan Jeyaraj and Nadar, 2019) designed an automatic physiological smart signal monitoring system. In addition to monitoring the patients for a long time, the authors applied estimation algorithms and deep neural network-based signal prediction to increase the prediction accuracy in smart monitoring. However, security and scalability were ignored.

Laplante et al. (Laplante et al., 2018) designed a systematic method to begin the process of eliciting requirements for an HIoT-based care system and to support emergency room activities at hospitals. They showed that this method could be generalized to identify boundaries and stakeholders for a broader HIoT application covering the entire hospital. Jeong and Shin (2018) suggested healthcare services in which IoT devices were installed in a vehicle to transport patients to the health centers while the ambulances are inaccessible. Hence, the proposed model enabled the hospital to accurately identify the patient's health conditions in real-time caring before the patient arrived. Also, Ghasemi, et al. (Ghasemi et al., 2019) designed an HIoT-based smart home architecture to decrease the cost of elderly care and medicine. According to this design, QoS, availability, performance, security, and interoperability requirements were satisfied.

Yang et al. (Yanget al., 2018) proposed a rule-based and adaptive lifelogging physical activity validation model for eliminating data reliability and irregular uncertainties in personalized HIoT-based environments. Further, Onasanya, et al. (Onasanya et al., 2019) designed the smart Saskatchewan healthcare system in four services, including cloud services and business analytics, emergency services, cancer care services, and operational services based on IoT technologies especially WSN, and other connected devices for long-term caring that employed a full-mesh hierarchical network topology to preserve the security and privacy with low power consumption.

Moreover, Vedaei, et al. (Vedaeiet al., 2020) designed a framework that captures health parameters, updates user health conditions, and considering COVID-19 environmental risk, notifies users to maintain physical distance. Sharma et al. (Sharma et al., 2020) proposed a framework based on deep learning and IoT to detect Alzheimer patients, track their activities, and provide them with a different type of assistance via IoT devices. Bandopadhaya et al. (Bandopadhaya et al., 2020) integrated IoT and distributed computing to monitor soldier's health conditions and initiate necessary medical treats soonest possible.

5.4.1.2. Recommender systems. In addition to monitoring systems, recommender systems suggest appropriate medicine or food based on patients' strict diets, including (Ullah et al., 2017), (Aliet al., 2018), (Subramaniyaswamyet al., 2018), (Lin et al., 2019), (Asghari et al., 2019b), and (Gope et al., 2020).

Ullah et al. (Ullah et al., 2017) proposed semantic interoperability of the big data model for the heterogeneous IoT devices to capture users' diseases symptoms and recommend drugs along with their side effects. Ali et al. (Aliet al., 2018) designed an IoT-based healthcare system for long-term care and proposed an efficient fuzzy ontology-based and type-2 fuzzy logic decision-making knowledge-based recommendation system to extract patient risk factors and diabetes prescriptions. Further, this system prevents unauthorized access to patients' information. The performance, accuracy of prediction, and precision of recommendation were evaluated to validate this system. Subramaniyaswamy et al. (Subramaniyaswamyet al., 2018) introduced a travel recommender system to support travelers following strict diets and have long-term diseases. Moreover, hybrid filtering mechanisms were applied to suggest appropriate recommendations along with intelligent recommendation models with high accuracy and stability.

Lin et al. (Lin et al., 2019) suggested a home healthcare matching service to meet the patients' needs based on their priorities and pre-defined rule-based logic. The authors tried to implement a system to recommend a service to the patients based on their needs and preferences, but the security and performance of this service were ignored. Asghari et al. (Asghari et al., 2019b) introduced a monitoring system to

Table 10
The selected application-based approaches and their information.

Scope		Article	Main idea	Evaluation technique(s)	Tool(s) and evaluation environment(s)	Advantage(s)	Disadvantage(s)
Monitoring systems	Prediction systems	Verma and Sood (2018)	An IoT cloud-based disease diagnosis framework in healthcare	Simulation	Python, WEKA	➢High accuracy ➢High sensitivity ➢High specificity ➢High F-Measure	➢Low scalability
		Kumar et al. (2018)	An IoT and cloud-based disease prediction system	Real testbed	UCI repository, Java	➢High performance ➢Low latency	➢Low security
		(Sood and Mahajan, 2019)	An IoT-fog based healthcare monitoring for hypertension attack	Simulation	WEKA 3.7	➢High efficiency ➢High accuracy ➢Low latency ➢Low BW utilization	➢Low security ➢Low privacy ➢Low scalability
		Verma et al. (2018)	A cloud-centric student waterborne diseases framework in HIoT	Simulation	MySQL, WEKA 3.6, TOMCAT	➢High accuracy ➢High sensitivity ➢High performance ➢Low latency	➢Low scalability
		Kaur et al. (2019)	Random forest techniques in HIoT for monitoring and predicting diseases	Real testbed	WEKA	➢High accuracy ➢High efficiency	➢Low security ➢Low scalability
		Suresh et al. (2019)	A real-time monitoring framework using a classifier for HIoT systems	Simulation	Not mentioned	➢High accuracy ➢High optimization ➢Low latency	➢Low security ➢Low privacy ➢Low scalability
		Tan and Halim (2019)	An HIoT predicting system using ANN classification models	Prototype	UCI repository	➢High accuracy ➢Low latency	➢Low security ➢Low privacy ➢Low scalability
		Rajan et al. (2020)	Atrial fibrillation classification in HIoT using a deep learning algorithm	Prototype	MATLAB, LabVIEW,	➢High accuracy ➢High sensitivity ➢High performance	➢Low security ➢Low scalability
		Satpathy et al. (2019)	A fuzzy classifier diagnosis system using FPGA	Simulation	MATLAB	➢High accuracy ➢High sensitivity ➢Low latency	➢Low security ➢Low scalability
		Bhatia et al. (2020)	An IoT-based system to predict Diabetes based on Urine	Simulation	iFogSim	➢Low latency ➢High efficiency ➢High reliability ➢High stability ➢High accuracy	➢High energy ➢Low scalability
		Vedaraj and Ezhumalai (2020)	A secure IoT-based architecture to predict diseases	Real testbed	Java, MySQL	➢High performance ➢Low computation cost ➢High accuracy ➢High security	➢Low robustness
		Fouad et al. (2020)	Using IoT and AI to predict the patient's health condition	Simulation	MATLAB	➢High accuracy ➢High precision	➢High maintenance cost
		Akhbarifar et al. (2020)	Secure health monitoring system using block encryption and data mining	Real testbed	C#, Weka 3.6	➢High precision ➢High accuracy ➢High f-score ➢High security ➢High confidentiality	➢Low throughput
	Detection systems	Azimiet al. (2017)	A fog-based hierarchical architecture for arrhythmia & CVDs detection	Real testbed	Python	➢High performance ➢High security ➢High accuracy ➢High reliability ➢High QoS ➢Low latency ➢Low BW utilization	➢High energy ➢Low scalability
		Jebadurai and Dinesh Peter (2018)	A super-resolution of retinal images algorithm in IoT which used multi-kernel SVR in healthcare	Real testbed	Welch Allyn iExaminer	➢High performance ➢High reliability	➢Low security ➢Low privacy ➢Low scalability
		Khowaja et al. (2018)	A framework for stress and fall detection using wearable sensors	Real testbed	Android 4.3	➢High accuracy ➢High security ➢High mobility ➢Low cost ➢Low latency	➢Low privacy ➢Low scalability

(*continued on next page*)

Table 10 (*continued*)

Scope	Article	Main idea	Evaluation technique(s)	Tool(s) and evaluation environment(s)	Advantage(s)	Disadvantage(s)
	Tuliet al. (2020)	A smart fog-based healthcare system for automatic diagnosis of heart diseases	Real testbed	Python	➢High accuracy ➢High QoS ➢Low energy ➢Low latency ➢Low BW utilization	➢High cost ➢Low security ➢Low privacy
	Alam et al. (2019)	Affective state mining in HIoT	Real testbed	Python 3.0, Torch 7.0	➢High accuracy ➢High performance	➢Low security ➢Low scalability
	Alhussein et al. (2018)	Seizure detection and monitoring in CHIoT	Simulation	PyTorch	➢High accuracy ➢High sensitivity ➢Low latency	➢Low security ➢Low privacy ➢Low reliability ➢Low scalability
	Rajan et al. (2020)	A fog-based HIoT system using deep neural networks for oral cancer detection	Simulation	Not mentioned	➢High accuracy ➢High sensitivity ➢Low latency	➢Low security ➢Low privacy ➢Low scalability
	Ray et al. (2018)	Fruit ripening detection for IoT based e-healthcare	Formal	Not mentioned	➢Low latency ➢Low cost	➢Low scalability ➢Low security
	Hosseinzadehet al. (2020b)	IoT based elderly health monitoring system	Simulation	Weka 3.6	➢High accuracy ➢High precision ➢High recall ➢High f-score ➢Low execution time	➢Low robustness
	Zgheib et al. (2020)	Using semantic reasoning technique and IoT for early epidemic detection	Simulation	ADLSim	➢High scalability ➢Real-time detection ➢High performance	➢Imprecise queries and models ➢Low privacy
	Rahmani et al. (2020)	An architecture for data analysis of IoT-based healthcare applications	Simulation	NEspr, MySQL, MATLAB	➢High accuracy ➢High integrity ➢High reliability ➢High dependability ➢Low cost	➢Low usability
	AbdulGhaffar et al. (2020)	An IoT-based system to monitor multiple diseases	Simulation	Cisco Packet Tracer Simulator Tool	➢High performance ➢High stability	➢Low security ➢Low scalability ➢Low functionality
	Kesavan and Arumugam (2020)	The neural network-based health monitoring system in IoT environment	Simulation	Not mentioned	➢High accuracy ➢High efficiency ➢Low response time ➢Low computational cost ➢High performance	➢Low privacy ➢Low scalability
	Kavitha and Ravikumar (2020)	The health monitoring system, a combination of IoT, machine learning, and neural network	Simulation	OMNeT++	➢High accuracy ➢High scalability ➢Low network latency ➢Low response time	➢Low privacy
Care-support systems	Jabbar et al. (2017)	A semantic interoperability model for HIoT heterogeneous infrastructures	Simulation	Gruff-6.2.0, MySQL, SPARQL, Tableau	➢High interoperability ➢High performance	➢Low security
	Rahmaniet al. (2018)	A smart e-healthcare gateway fog-based architecture for monitoring	Real testbed	Python, MySQL	➢High mobility ➢High security ➢High reliability ➢High interoperability ➢Low energy	➢Low scalability
	Laplante et al. (2018)	A structured framework for describing, designing, and implementing healthcare IoT systems	Design	Not mentioned	➢High stability	➢Low security ➢Low interoperability
	Ramírez López et al. (2019)	An IoT-based monitoring system for respiratory disorders	Real testbed	Rpi3B, Arduino	➢High performance ➢High accuracy ➢Low energy ➢Low latency	➢Low scalability

(*continued on next page*)

Table 10 (*continued*)

Scope	Article	Main idea	Evaluation technique(s)	Tool(s) and evaluation environment(s)	Advantage(s)	Disadvantage(s)
	Onasanya and Elshakankiri (2019)	An IoT/WSN-based care service	Real testbed	Hadoop	➢Low cost ➢High security ➢High availability ➢High reliability ➢Low overhead	➢Low scalability
	Rajan Jeyaraj and Nadar (2019)	Smart monitoring using deep learning in HIoT	Prototype	Weka	➢High accuracy ➢High reliability	➢Low security ➢Low scalability
	Laplante et al. (2018)	The process of eliciting requirements for HIoT applications	Prototype	UML	➢High security ➢High efficiency	➢Low scalability
	Jeong and Shin (2018)	HIoT applications in the vehicle using implantable devices	Simulation	Not mentioned	➢High efficiency ➢High reliability ➢Low overhead	➢Low scalability
	Ghasemi et al. (2019)	An HIoT-based smart home architecture	Design	ATAM	➢High privacy ➢High security ➢High performance ➢High availability ➢Low latency	➢Low scalability
	Yanget al. (2018)	Data validation for lifelogging physical activities in HIoT	Real testbed	MATLAB	➢High efficiency ➢High interoperability ➢High reliability ➢High performance	➢Low scalability
	Onasanya et al. (2019)	Smart Saskatchewan healthcare system based on IoT and WSN	Real testbed	Not mentioned	➢High security ➢Low energy	➢Low scalability
	Vedaeiet al. (2020)	IoT based monitoring system to care against COVID-19 pandemic	Real testbed	Not mentioned	➢Low cost ➢Lightweight computations ➢Low energy	➢Low scalability ➢Low privacy ➢Low security
	Sharma et al. (2020)	A framework based on deep learning and IoT to assist Alzheimer patients	Simulation	Not mentioned	➢High accuracy ➢High precision ➢High F-score ➢High recall ➢High scalability	➢Moderate performance ➢Low privacy ➢Low security
	Bandopadhaya et al. (2020)	Using IoT and distributed computing to monitor healthcare of soldiers	Prototype	Temperature sensor (MAX30205), Dragino LoRa transceiver	➢High speed ➢Low processing time ➢High scalability ➢High load balancing ➢High performance	➢Low privacy
Recommender systems	Ullah et al. (2017)	A semantic interoperability model for big data for heterogeneous devices in HIoT	Simulation	Gruff-6.2.0, MySQL, SPARQL, Tableau	➢High interoperability	➢Low security
	Aliet al. (2018)	A recommendation system using type-2 fuzzy ontology–aided in HIoT	Design	MATLAB, SPARQL, Protégé OWL-2	➢High security ➢High accuracy ➢High efficiency	➢Low privacy ➢Low scalability
	Subramaniyaswamyet al. (2018)	A fog-based food recommendation system for travelers in IoT healthcare	Design	Not mentioned	➢High accuracy ➢High stability ➢High F-Measure ➢High Recall ➢Low latency	➢Low mobility ➢Low security ➢Low scalability
	Lin et al. (2019)	A home healthcare IoT-based matching service	Real testbed	Not mentioned	➢Low latency ➢Low cost	➢Low security ➢Low scalability
	Asghari et al. (2019b)	HIoT-based monitoring, predicting, and composition services	Simulation	Weka 3.6	➢High accuracy ➢High efficiency ➢High security ➢Low latency ➢Low cost	➢Low scalability
	Gope et al. (2020)	IoT-based healthcare monitoring system with decision making	Simulation	JCE library, AVISPA	➢High security ➢High efficiency ➢High privacy	➢Low integrity

Table 11
A comparison of the evaluation factors in the application-based approaches.

Scope		Article	Security	Privacy	Accuracy	Performance	Reliability	Interoperability	Time	Cost	Energy
Monitoring systems	Prediction systems	Verma and Sood (2018)			*	*					
		Kumar et al. (2018)				*			*		
		Sood and Mahajan (2019)			*	*			*		
		Verma et al. (2018)			*	*			*		
		Kaur et al. (2019)			*	*					
		Suresh et al. (2019)			*	*			*		
		Tan and Halim (2019)			*				*		
		Rajan et al. (2020)			*	*					
		Satpathy et al. (2019)			*	*			*		
		Bhatia et al. (2020)			*	*	*		*		
		Vedaraj and Ezhumalai (2020)	*		*	*				*	
		Fouad et al. (2020)			*						
		Akhbarifar et al. (2020)	*		*						
	Detection systems	Azimiet al. (2017)	*		*	*	*		*		
		Jebadurai and Dinesh Peter (2018)				*	*				
		Khowaja et al. (2018)	*		*	*			*	*	
		Tuliet al. (2020)			*	*			*		*
		Alam et al. (2019)			*	*					
		Alhussein et al. (2018)			*				*		
		Rajan et al. (2020)			*				*		
		Ray et al. (2018)							*	*	
		Hosseinzadehet al. (2020b)			*				*		
		Zgheib et al. (2020)				*			*		
		Rahmani et al. (2020)			*		*			*	
		AbdulGhaffar et al. (2020)				*					
		Kesavan and Arumugam (2020)			*	*			*	*	
		Kavitha and Ravikumar (2020)			*				*		
	Care-support systems	Jabbar et al. (2017)				*		*			
		Rahmaniet al. (2018)	*				*	*			*
		Laplante et al. (2018)					*				
		Ramírez López et al. (2019)	*	*	*	*	*		*	*	*
		Onasanya and Elshakankiri (2019)	*				*				
		Rajan Jeyaraj and Nadar (2019)			*	*	*		*		
		Laplante et al. (2018)	*	*		*					
		Jeong and Shin (2018)				*	*				
		Ghasemi et al. (2019)	*	*		*			*		
		Yanget al. (2018)				*	*	*			
		Onasanya et al. (2019)	*								*
		Vedaeiet al. (2020)							*	*	*
		Sharma et al. (2020)			*						
		Bandopadhaya et al. (2020)				*			*		
Recommender systems		Ullah et al. (2017)						*			
		Aliet al. (2018)	*		*	*					
		Subramaniyaswamyet al. (2018)			*		*		*		
		Lin et al. (2019)							*	*	
		Asghari et al. (2019b)	*	*	*	*			*	*	
		Gope et al. (2020)	*	*		*					

predict and diagnose some determined diseases; afterward, they recommended an appropriate health/medical service composition to meet the patients' preferences, such as location, time, and cost limitations. This framework is an accurate, efficient, secure, and privacy preserver based on the experimental results. Moreover, Gope, et al. (Gope et al., 2020) designed authentication and fault-tolerant decision-making schemes to construct an IoT-based healthcare system.

5.4.2. A summary of application-based approaches

Monitoring and recommender systems are introduced in application-based approaches to predict and detect anomaly situations or observe the patients for a long time and recommend appropriate medicine to them. The application-based approaches along with significant ideas, the evaluation techniques and tools, and other information, are presented in Table 10. Additionally, Table 11 offers a comparison of some factors such as security, privacy, and accuracy.

5.5. Security-based approaches

Security-based approaches are the last category in the proposed categorization that addresses such aspects of a secure HIoT system as privacy, access control, confidentiality, and trust to provide the QoS in HIoT. Moreover, the security-based articles are reviewed in Section 5.5.1, and applied techniques and tools in the articles and the comparison between them are summarized in Section 5.5.2.

5.5.1. An overview of the selected security-based approaches

This section presents an overview of the selected security-based approaches in four categories as follows.

5.5.1.1. Privacy. The security-based articles focusing on privacy issue are (Boussada et al., 2019), (Elmisery et al., 2016), (Saha et al., 2019), (Tao et al., 2019), (Jiang et al., 2019), (Tang et al., 2019), (Baek et al., 2016), (Elmisery et al., 2017), (Li et al., 2018), (Rani et al., 2019), (Hamza et al., 2020), and (Guo et al., 2020).

Boussada et al. (Boussada et al., 2019) suggested a privacy-preserving HIoT scheme and a lightweight identity-based encryption algorithm to provide privacy, data integrity, and authentication. Experimental results showed the efficiency, privacy-preserving, and low transmission delay of the scheme. Elmisery et al. (Elmisery et al., 2016) presented a privacy-based fog middleware for HIoT that kept the accuracy adopted from cloud-based healthcare recommended service. The authors claimed that this model needed to use game theory to have better groups of HIoT devices. Saha et al. (Saha et al., 2019) proposed an e-healthcare framework that deal with electronic medical records and preserved privacy. The authors proved the high performance and efficiency of the proposed framework in terms of time, memory consumption, latency, and response time; however, the reliability issue was not addressed. Tao et al. (Tao et al., 2019) proposed a secure data collection scheme for HIoT applications that protects users' privacy. In addition, to validate the scheme, KATAN, and secret cipher share algorithms were simulated to show energy cost, hardware frequency rate, and computation time of the scheme. One of the advantages of this method is its distributed cloud computing architecture that prevents the single point of failure, but this scheme suffers from high complexity and overhead. Jiang et al. (Jiang et al., 2019) implemented a privacy-preserving diabetic retinopathy detection system. The authors illustrated the provision of privacy-preserving homomorphic surf and fast multi-retina-image matching methods. The proposed system has efficient point detection for retinal images of diabetic retinopathy; however, limited homomorphic comparison schemes were applied in experimental results.

Tang et al. (Tang et al., 2019) introduced a multi-source health data aggregation scheme that supports high-level privacy preservation and is resistant to differential attacks. Additionally, the security, fault tolerance, and performance in terms of cost-efficiency, computation time, communication, and storage overhead were evaluated; however, only differential and replay attacks were considered.

Baek et al. (Baek et al., 2016) presented a mobile healthcare system with high privacy and security over the cellular network to help mobile users to communicate anonymously. The system is resistant to some popular attacks such as eavesdropping, matching, replay, collusion, and impersonation attacks. The system also provides unlinkability between the patients' nicknames and their real identifications in all communications. According to the experimental results, the system is efficient in communication traffic management; however, the constrained battery lifetime of mobile devices has been ignored.

Elmisery et al. (Elmisery et al., 2017) presented a fog middleware for collective privacy in HIoT-based cloud healthcare services that preserves privacy. Experiments showed that the mechanism supported accuracy with high privacy and performance. However, the mechanism is vulnerable to shilling attacks. Li et al. (Li et al., 2018) introduced (a, k)-anonymity model as a privacy-preserving scheme for data collection in healthcare services. Additionally, to the validate proposed scheme, the authors used adult datasets from the UCI machine-learning repository with high privacy, efficiency, and low execution time. Rani et al. (Rani et al., 2019) presented a healthcare data security scheme to provide high security and privacy using the SIMON block cipher algorithm and shared generation model. Experimental results showed the efficiency and performance of the scheme in terms of energy cost, throughput, response time, execution time, and latency; however, the scheme just used specific and limited algorithms. Hamza et al. (Hamza et al., 2020) proposed fast encryption based on probabilistic cryptosystem (chaos-based) to preserve the privacy of patients' images against different attacks and securely transmit diagnostically images to medical specialists. Finally, Guo, et al. (Guo et al., 2020) presented a data clustering strategy along with hemimorphic encryption to efficiently cluster the data while preserving participants' mutual privacy and keeping secret their private data.

5.5.1.2. Access control. Another category of the selected articles is related to the access control and includes two subcategories namely authorization (Pal et al., 2019), (Yang et al., 2019), (Yang et al., 2018), (Xu et al., 2019) and authentication (Aghili et al., 2019), (Arfaoui et al., 2019), (He and Zeadally, 2015), (Yeh, 2016), (Al-Turjman and Alturjman, 2018), (Deebak et al., 2019), (Huang et al., 2019), (Karimian et al., 2019), (Hou and Yeh, 2015), (Kumar and Gandhi, 2017), (Zhou and Piramuthu, 2018), (Jia et al., 2018), (Karthigaiveni and Indrani, 2019), (Merabet et al., 2019), (Sharma and Kalra, 2019), (Benadda et al., 2018), (Vaishnavi and Sethukarasi, 2020), (Alzahrani, 2020), (Sun et al., 2020), (Gupta et al., 2020), (Xu, 2020), (Alladi and ChamolaNaren, 2020), (Sun et al., 2020), (Sahoo et al., 2020), (Fotouhi et al., 2020), (Islam and Young Shin, 2020).

Pal et al. (Pal et al., 2019) introduced a policy-based access control to protect constrained resources in HIoT from unauthorized access. Moreover, the authors used a decentralized architecture to reduce response time. Yang et al. (Yang et al., 2019) presented a privacy-preserving HIoT-based system along with self-adaptive access control for the authorized users in normal situations and emergencies. Simulation results showed that the system outperformed in terms of performance, efficiency, security, and computational cost. Yang et al. (Yang et al., 2018) introduced a lightweight data sharing system for authorized data users that supported attribute-based and break-glass access to encrypted medical records with low computational and communicational overheads. Xu et al. (Xu et al., 2019) proposed a healthcare IoT system that includes attributed-based encryption for authorized data, cloud and fog computing, and secure fine-grained access control with lightweight decryption. Experiments showed that the performance of the system was better than other schemes.

Aghili et al. (Aghili et al., 2019) introduced an ownership transfer and lightweight, energy-efficient, and secure authentication protocol for HIoT systems. The protocol provided access control and preserved privacy; however, the hardware cost was not optimized.

Arfaoui et al. (Arfaoui et al., 2019) presented a lightweight and context-aware anonymous authentication and key agreement method for WBAN applications in normal and emergency situations. By using the NS2 simulator, the model was validated to show its high efficiency and low overhead. However, there was not a tradeoff between security and energy consumption. He and Zeadally (2015) presented the security requirements of RFID authentication methods and a review of elliptic curve cryptography (ECC)-based RFID authentication methods in terms of security and performance in the healthcare environment. Eventually, the proposed ECC-based RFID authentication method had acceptable computation and communication costs, and all the security requirements were satisfied.

Yeh (2016) presented two secure authentication schemes for IoT-based healthcare, relying on body sensor networks (BSNs). The feasibility and practicability of the presented schemes were proved by using Raspberry PI platform. Furthermore, the proposed schemes are suitable to implement common intelligent mobile objects with robust security density and confidentiality. However, the suggested schemes are vulnerable to SHA-2 attack. Al-Turjman and Alturjman (2018) proposed a context-sensitive identity-provisioning framework for the industrial HIoT using wireless sensor networks along with a secure mutual authentication approach. The framework was resilient to some known attacks and was suitable for real-time applications. Simulation results

showed its high-performance efficiency with low overhead and bandwidth usage. Despite all advantages of the framework, its major weak point was low reliability.

Deebak et al. (Deebak et al., 2019) proposed a secure biometric-based user authentication scheme to reduce computation and communication cost and storage to improve the performance of any real-time-based healthcare application systems. Huang et al. (Huang et al., 2019) introduced a lightweight authentication scheme for noisy ECG signals to provide more efficient privacy protection. The scheme was compared with other schemes to prove its high accuracy and reliability. However, only two data sets were used to analyze the proposed scheme. Karimian et al. (Karimian et al., 2019) proposed a noise-aware biometric key generation/authentication framework that outperformed other deep-learning-based access control and data protection schemes in terms of reliability, cost, energy, accuracy, and performance. Although the security and privacy aspects were considered, the framework was vulnerable to some attacks.

Hou and Yeh (2015) designed a secure authentication model for IoT-based healthcare. Indeed, the model included an authentication-based sign-on technique and a one-way hash function with a random nonce to ensure system security robustness and efficiency. Further, the model was resistant to replay and forgery attacks. Kumar and Gandhi (2017) introduced smart gateway-based authorization and authentication scheme to protect sensitive physiological data against malicious users and attackers. Zhou and Piramuthu (2018) presented a flexible technology in a supply chain with a sample of RFID implementation in a health care service. This adaptive knowledge-based system could switch between authentication protocols based on environmental characteristics, and it had the capability to learn from its mistakes. Jia et al. (Jia et al., 2018) proposed an authenticated key agreement scheme for fog-driven applications based on bilinear pairings and elliptic curve groups. The scheme was robust against some popular attacks such as stolen smart card attacks, replay attacks, and its security was proved in the random oracle model. In addition, the performance of the scheme was validated in terms of computation and communication costs. However, the use of mathematical algorithms, including the elliptic curve cryptography, caused overhead, complexity, and low efficiency. Karthigaiveni and Indrani (2019), using elliptic curve cryptography and smart card, proposed an efficient password along with two-factor authentication scheme for HIoT. Based on the analysis of the scheme in random oracle model, the scheme was secure with low computational and communication costs; however, the privacy issue was ignored.

Merabet et al. (Merabet et al., 2019) presented three efficient and lightweight authentication protocols for IoT-based healthcare applications. Two of them were suitable for the machine-to-cloud communication mode, and the last one was for the machine-to-machine mode. According to the experimental results, these authentication protocols outperformed in terms of performance. Sharma and Kalra (Zhou and Piramuthu, 2018) presented a secure authentication scheme for real-time remote patient monitoring, which was lightweight, robust, and reliable against multiple security attacks. AVISPA simulation tool was applied to validate the security and efficiency of the scheme. Benadda et al. (Benadda et al., 2018) implemented a secure HIoT-based wearable framework to monitor elderlies' motions. The authors considered hardware implementation before software running. In this regard, the authentication chip ATSHA204A was used to generate a unique identification code, and then it was combined with cryptographic protocols to satisfy the security requirements.

Vaishnavi and Sethukarasi (2020) proposed an authentication scheme including a lightweight encryption algorithm to transmit health records securely and a novel detection algorithm to detect suspicious users as Sybil nodes and broadcast the list of them. Alzahrani (2020), using symmetric key encryption, the proposed authentication and key agreement scheme for medical information systems improved authenticity. Sun et al. (Sun et al., 2020) proposed an optimized vector transformation method to design a privacy-preserving lightweight access control policy for smart HIoT that eliminates the burden of encryption, decryption, and key generation. Gupta et al. (Gupta et al., 2020) presented an access control and authentication scheme based on lattice for HIoT systems that mitigate several attacks. Xu (2020) presented an IoT-assisted framework to securely transmit data, enforcing access control, analyze ECG signal strength, and monitor cardiovascular health continuously.

Furthermore, Alladi, et al. (Alladi and ChamolaNaren, 2020) leveraged hardware security functionalities and proposed a lightweight two-way authentication protocol, which takes into account the IoT devices energy and memory constraints. Sun et al. (Sun et al., 2020) integrated SDN and edge computing to propose a secure framework that edge servers authenticate IoT devices, and then these devices could collect and send the patients' data to edge servers. Sahoo et al. (Sahoo et al., 2020) used ECC and presented a key agreement and three-factor authentication scheme. It provides security, mutual authentication, and user anonymity along with low computational and communication cost. Fotouhi et al. (Fotouhi et al., 2020) proposed an authentication scheme based on the hash chain for WBANs in HIoT that provides security and authenticity with low computational and storage cost. Finally, Islam and Young Shin (Islam and Young Shin, 2020) proposed a secure healthcare design based on blockchain that provides some security features.

5.5.1.3. Confidentiality. Another category of the selected articles is related to the Confidentiality that concentrates on encryption techniques of health data, including (Kaw et al., 2019), (EL-Latif et al., 2020), (Li and Jing, 2019), (Elhoseny et al., 2018), (Ming et al., 2020), and (Ullah et al., 2020a).

Kaw et al. (Kaw et al., 2019) proposed a secure framework using information hiding in encrypted images approach to ensure client data security and prevent unauthorized access to client data. This study improved computational cost and security issues. EL-Latif et al. (EL-Latif et al., 2020) proposed an image-encryption-based method for controlled alternate quantum walks (CAQWs) to preserve the privacy of healthcare images in IoT; efficiency and security of the method were proved by simulation and numerical analysis. Li and Jing (2019) designed a hybrid IoT-fog-cloud framework in which fog was distributed between the IoT devices and cloud to overcome resource limitations and meet storage, security, and privacy requirements. Furthermore, the framework used keyword-searchable encryption with fine-grained access control. Elhoseny et al. (Elhoseny et al., 2018) proposed a secured medical data transmission approach based on integrating hybrid blending AES, steganography, and RSA encryption techniques to reach high reliability and capacity imperceptibility and minimal deterioration. Ming et al. (Ming et al., 2020) combined certificate-based cryptography and ECC and proposed an efficient signcryption scheme based on certification, which provides anonymity, confidentiality, privacy, unforgeability. Ullah et al. (Ullah et al., 2020a) presented a certificate-based signcryption and encryption scheme for HIoT that provides signature, encryption, unforgeability, confidentiality, security while reducing communication and computation cost.

5.5.1.4. Trust. The last class of articles in security-based methods attempts to satisfy trust requirements, including (Manogaran et al., 2018), (Gope and Hwang, 2016), (Ullah et al., 2020b), (Rathee et al., 2019), (Abou-Nassar et al., 2020), and (Amin et al., 2020).

Manogaran et al. (Manogaran et al., 2018) presented the architecture of HIoT systems to store, process, and analyze big data in BSN with concentrating on security aspects. Additionally, this architecture used a MapReduce-based prediction model to predict heart diseases. Gope and Hwang (2016) described security and privacy scheme in BSN healthcare applications, called BSN-Care, to accomplish efficiently various security requirements of BSN-based healthcare systems. Ullah et al. (Ullah et al.,

Table 12
The selected security-based approaches and their information.

Scope			Article	Main idea	Evaluation technique(s)	Tool(s) and evaluation environment(s)	Advantage(s)	Disadvantage(s)
Security	Privacy		Boussada et al. (2019)	A privacy-preserving HIoT scheme	Simulation	AVISPA	➢High efficiency ➢High privacy ➢High interoperability ➢Low latency ➢Low energy	➢Low scalability
			Elmisery et al. (2016)	A secure privacy-based system on a fog middleware in HIoT	Prototype	C++, MySQL	➢High privacy ➢High security ➢High accuracy	➢Low scalability ➢Vulnerable to some attacks ➢Low optimization
			Saha et al. (2019)	Privacy-preserving in IoT healthcare by fog-enhanced applications	Real testbed	LINDDUN	➢High performance ➢High efficiency ➢Low latency	➢Low scalability
			Tao et al. (2019)	A secure hardware-based data collection in HIoT	Real testbed	Python	➢High security ➢Low latency ➢Low energy	➢High complexity ➢High overhead ➢Low scalability
			Jiang et al. (2019)	A privacy-preserving scheme for diabetic retinopathy detection in HIoT	Real testbed	Raspberry Pi Noir, Camera V2	➢ High privacy ➢High security ➢High performance ➢Low latency	➢Low scalability
			Tang et al. (2019)	A privacy-preserving e-health data aggregation scheme in IoT	Design	Not mentioned	➢High privacy ➢High reliability ➢Low latency ➢Low overhead	➢Low security
			Baek et al. (2016)	A privacy-enhanced mobile healthcare system	Real testbed	Nexus 5	➢High privacy ➢High security ➢High efficiency	➢High energy
			Elmisery et al. (2017)	A privacy-preserving fog-based middleware in HIoT	Real testbed	MySQL, C++	➢High accuracy ➢High efficiency ➢High privacy ➢Low latency	➢Low optimization ➢Low scalability
			Li et al. (2018)	Privacy-preserving by (a, k)-anonymous schemes in smart healthcare	Real testbed	UCI repository	➢High efficiency ➢High privacy ➢Low latency ➢Low overhead	➢Low reliability
			Rani et al. (2019)	Secure data transmission in HIoT with the lightweight block cipher	Real testbed	Java	➢High security ➢High privacy ➢High optimization ➢Low latency ➢Low energy	➢Low scalability
			Hamza et al. (2020)	Privacy-preserving and secure data transmission in HIoT, using encryption	Simulation	MATLAB	➢High security ➢High privacy ➢Low energy ➢Low communication overhead ➢High speed ➢High confidentiality ➢Low latency	➢Low efficiency ➢Low access control
			Guo et al. (2020)	A privacy-preserving data clustering in HIoT	Formal Simulation	Python	➢ High privacy ➢ High security ➢ High accuracy	➢High communication complexity ➢Low scalability
	Access control	Authorization	Pal et al. (2019)	Policy-based access control for constrained resources in HIoT	Real testbed	Not mentioned	➢High performance ➢High security ➢Low latency ➢Low overhead	➢Low scalability ➢High energy
			Yang et al. (2019)	An IoT-based privacy-preserving and access control for big data in HIoT	Simulation	C, Visual studio	➢High security ➢High performance ➢Low energy ➢Low overhead	➢Low scalability
			Yang et al. (2018)	Lightweight access control in healthcare for IoT	Simulation	Not mentioned	➢High performance ➢Low overhead	➢Low scalability
			Xu et al. (2019)	A lightweight privacy-preserving scheme in HIoT	Simulation	Java	➢High performance	➢Low scalability

(*continued on next page*)

Table 12 (*continued*)

Scope		Article	Main idea	Evaluation technique(s)	Tool(s) and evaluation environment(s)	Advantage(s)	Disadvantage(s)
						➢High security ➢High privacy ➢Low latency	
	Authentication	Aghili et al. (2019)	An ownership transfer and lightweight authentication protocol for HIoT	Formal	Not mentioned	➢High security ➢High privacy ➢High performance ➢Low energy	➢High cost ➢High overhead ➢Low integrity
		Arfaoui et al. (2019)	A lightweight and context-aware anonymous authentication and key agreement scheme for WBAN applications	Simulation	NS2 2.35, Scyther	➢High security ➢High efficiency ➢Low overhead ➢Low complexity	➢High energy
		He and Zeadally (2015)	An RFID authentication scheme for IoT in healthcare systems	Formal	Not mentioned	➢High confidentiality ➢High availability ➢High security ➢High scalability ➢Low cost ➢Low overhead	➢Vulnerable to some attacks
		Yeh (2016)	A secure body sensor network architecture in HIoT	Simulation	Raspberry PI	➢High efficiency ➢High confidentiality	➢Vulnerable to SHA-2 or 3 attacks ➢High overhead
		Al-Turjman and Alturjman (2018)	A context-sensitive seamless identity scheme for industrial IoT healthcare	Simulation	MIRACLE, C/C++,	➢High performance ➢High security ➢Low overhead ➢Low bandwidth utilization	➢ Low scalability (resilient against some specific attack)
		Deebak et al. (2019)	An authentication scheme for smart healthcare in IoT	Simulation	NS3	➢High performance ➢High security ➢Low latency ➢Low overhead	➢ Low scalability
		Huang et al. (2019)	An authentication scheme for privacy-preserving the noisy ECG signals in HIoT	Real testbed	Python 2.7	➢High accuracy ➢High reliability ➢High efficiency ➢High security and privacy	➢ Low scalability
		Karimian et al. (2019)	A noise-aware biometric framework in HIoT	Real testbed	NTS	➢High reliability ➢High accuracy ➢Low latency ➢Low energy ➢Low cost	➢Low security
		Hou and Yeh (2015)	An HIoT-based authentication scheme	Formal	Not mentioned	➢High reliability ➢High security ➢High performance	➢Low scalability
		Kumar and Gandhi (2017)	A secure transmission protocol to preserve privacy in HIoT	Simulation	Contiki	➢High performance ➢High reliability ➢Low latency	➢Low scalability
		Zhou and Piramuthu (2018)	A secure flexible IoT healthcare framework	Simulation	Not mentioned	➢High efficiency ➢High accuracy ➢High sensitivity	➢Low optimization ➢Low mobility ➢Low scalability
		Jia et al. (2018)	Authentication for fog-driven smart healthcare applications	Simulation	Android 4.4.2	➢High performance ➢High mobility ➢High security ➢Low latency	➢High overhead ➢Low efficiency
		Karthigaiveni and Indrani (2019)	An efficient authentication scheme in HIoT	Simulation	Random oracle model	➢High security ➢Low latency ➢Low overhead	➢Low privacy ➢Low scalability
		Merabet et al. (2019)	Three M2M and M2C authentication protocols in HIoT	Real testbed	AVISPA, ProVerif	➢High security ➢High privacy ➢High performance ➢Low latency	➢ Low scalability
		Sharma and Kalra (2019)	A secure authentication scheme for real-time remote patient monitoring	Simulation	AVISPA	➢High security ➢High efficiency ➢Low latency ➢Low overhead	➢Low scalability
				Real testbed	Not mentioned	➢High security	➢Low scalability

(*continued on next page*)

Table 12 (*continued*)

Scope	Article	Main idea	Evaluation technique(s)	Tool(s) and evaluation environment(s)	Advantage(s)	Disadvantage(s)
	Benadda et al. (2018)	A secure HIoT-based wearable framework			➢Low energy	
	Vaishnavi and Sethukarasi (2020)	An authentication scheme to detect Sybil nodes	Simulation	NS3	➢High throughput ➢Low detection delay ➢High privacy ➢High security ➢Low cost ➢Timely detection	➢Low scalability ➢Low movability
	Alzahrani (2020)	An authentication and key agreement scheme for medical information systems	Simulation	ProVerif	➢High efficiency ➢High performance	➢Low security ➢No mutual authentication ➢No user anonymity ➢No untraceability ➢Low movability
	Sun et al. (2020)	Privacy-preserving access control for smart HIoT	Simulation	Java 8	➢High privacy ➢Low computation and storage cost ➢High efficiency ➢High security ➢Low cryptography time	➢Low traceability ➢Low scalability
	Gupta et al. (2020)	Lattice-based access control and authentication scheme	Simulation Formal	Not mentioned	➢High security ➢Low overhead	➢Low privacy
	Xu (2020)	ECG monitoring framework enforcing access control	Simulation, Formal	Not mentioned	➢High security ➢Low energy ➢High sensitivity ➢High efficiency ➢High accuracy ➢High reliability	➢Low privacy ➢Low scalability
	Alladi and ChamolaNaren (2020)	An authentication protocol for HIoT networks	Simulation, Formal	Raspberry	➢High security ➢High privacy ➢High Untraceability ➢High confidentiality ➢High integrity ➢Low computation cost	➢Low scalability
	Sun et al. (2020)	Authentication and transmitting data using a secure framework in HIoT systems	Simulation	MATLAB	➢Low response time ➢High packet delivery ratio ➢High throughput ➢Low overhead ➢Low delay	➢Low privacy
	Sahoo et al. (2020)	A three-factor authentication scheme based on ECC for HIoT systems	Simulation, Formal	AVISPA, BAN logic	➢High security ➢Low cost ➢Mutual authentication ➢User anonymity	➢Without considering nonrepudiation, unlinkability, and untraceability
	Fotouhi et al. (2020)	A secure authentication scheme based on hash-chain	Simulation Formal	OPNET ProVerif	➢High security ➢High untraceability ➢High efficiency ➢Low cost ➢Low storage ➢Sensor anonymity	➢Low scalability
	Islam and Young Shin (2020)	A secure healthcare design based on blockchain	Simulation, Real testbed	Not mentioned	➢High security ➢Low energy	➢Low performance ➢High latency ➢High cost
Confidentiality	Kaw et al. (2019)	Secure patient information hiding in HIoT systems	Formal	Not mentioned	➢High privacy ➢High security ➢High performance ➢Low overhead	➢High latency
	EL-Latif et al. (2020)	An image encryption mechanism based on CAQWs	Simulation	MATLAB	➢High security ➢High efficiency ➢High privacy	➢Low scalability
			Simulation	C	➢High security	➢ Low scalability

(*continued on next page*)

Table 12 (*continued*)

Scope	Article	Main idea	Evaluation technique(s)	Tool(s) and evaluation environment(s)	Advantage(s)	Disadvantage(s)
	Li and Jing (2019)	Lightweight searchable encryption in fog-based HIoT			➢High efficiency ➢Low storage ➢Low overhead ➢Low latency ➢Low energy	
	Elhoseny et al. (2018)	A hybrid security model for securing the diagnostic text data in medical images in IoT	Simulation	MATLAB	➢High security ➢High optimization ➢High stability ➢High performance	➢low scalability (used only AES and RSA)
	Ming et al. (2020)	Efficient anonymous signcryption scheme for HIoT	Formal	Not mentioned	➢High security ➢High privacy ➢High confidentiality ➢Unforgeability ➢Anonymity ➢Low computation ➢Low communication cost	➢ Low scalability
	Ullah et al. (2020a)	Secure and efficient signcryption scheme for mobile health systems	Formal	Not mentioned	➢High security ➢High confidentiality ➢Unforgeability ➢Low computation ➢Low communication cost	➢Low privacy ➢Low anonymity ➢Low scalability
Trust	Manogaran et al. (2018)	A new architecture for storing big health data for secured monitoring in HIoT	Real testbed	Not mentioned	➢High accuracy ➢High sensitivity ➢High specificity ➢High F-Measure ➢High Recall ➢High security	➢Low privacy ➢Low scalability
	Gope and Hwang (2016)	A modern secure and IoT-based body sensor network architecture	Simulation	Android 2.2	➢High performance ➢Low latency ➢Low overhead ➢Low energy	➢vulnerable to some attacks
	Ullah et al. (2020b)	Secure fog-based health data aggregation in IoT	Simulation	NS2 2.35	➢High performance ➢High security ➢Low energy ➢Low overhead	➢Low mobility ➢Low reliability
	Rathee et al. (2019)	A secure framework using blockchain techniques	Simulation	NS2	➢High security ➢High accuracy ➢High reliability	➢High cost ➢High latency
	Abou-Nassar et al. (2020)	A trust model using blockchain techniques	Simulation	C#	➢High security ➢High privacy ➢High confidentiality ➢High interoperability ➢High integrity ➢High scalability ➢High availability ➢High trustworthy	➢Low diagnosis accuracy ➢High cost ➢High latency
	Amin et al. (2020)	Malware detection in HIoT applications using deep learning	Simulation	Not mentioned	➢High security ➢High accuracy ➢High precision ➢High specificity ➢High f-score ➢High recall	➢Low scalability

Table 13
A comparison of the evaluation factors in the security-based approaches.

Scope			Article	Security	Privacy	Accuracy	Performance	Reliability	Scalability	Interoperability	Time	Cost	Energy
Security	Privacy		Boussada et al. (2019)	*	*		*			*	*		*
			Elmisery et al. (2016)	*	*	*							
			Saha et al. (2019)				*				*		
			Tao et al. (2019)	*							*		*
			Jiang et al. (2019)	*	*		*				*		
			Tang et al. (2019)	*	*		*				*		
			Baek et al. (2016)	*	*		*						
			Elmisery et al. (2017)		*	*	*				*		
			Li et al. (2018)		*		*				*		
			Rani et al. (2019)	*	*		*				*		*
			Hamza et al. (2020)	*	*						*		*
			Guo et al. (2020)	*	*	*							
	Access control	Authorization	Pal et al. (2019)	*	*		*				*		
			Yang et al. (2019)	*	*		*						*
			Yang et al. (2018)				*						
			Xu et al. (2019)	*	*		*				*		
		Authentication	Aghili et al. (2019)	*	*		*						*
			Arfaoui et al. (2019)	*	*		*						
			He and Zeadally (2015)	*					*			*	
			Yeh (2016)				*						
			Al-Turjman and Alturjman (2018)	*			*						
			Deebak et al. (2019)	*	*		*				*		
			Huang et al. (2019)	*	*	*	*	*					
			Karimian et al. (2019)			*		*			*	*	*
			Hou and Yeh (2015)	*			*	*					
			Kumar and Gandhi (2017)				*	*			*		
			Zhou and Piramuthu (2018)			*	*						
			Jia et al. (2018)	*			*				*		
			Karthigaiveni and Indrani (2019)	*							*		
			Merabet et al. (2019)	*	*		*				*		
			Sharma and Kalra (2019)	*	*		*				*		
			Benadda et al. (2018)	*	*								*
			Vaishnavi and Sethukarasi (2020)	*	*		*				*	*	
			Alzahrani (2020)				*						
			Sun et al. (2020)	*	*		*				*	*	
			Gupta et al. (2020)	*								*	*
			Xu (2020)	*		*	*	*					*
			Alladi and ChamolaNaren (2020)	*	*							*	
			Sun et al. (2020)				*				*	*	
			Sahoo et al. (2020)	*								*	
			Fotouhi et al. (2020)	*	*		*					*	
			Islam and Young Shin (2020)	*									*
	Confidentiality		Kaw et al. (2019)	*	*		*						
			EL-Latif et al. (2020)	*	*		*						
			Li and Jing (2019)	*	*		*				*		*
			Elhoseny et al. (2018)	*			*	*					
			Ming et al. (2020)	*	*						*	*	
			Ullah et al. (2020a)	*							*	*	

(*continued on next page*)

Table 13 (*continued*)

Scope	Article	Security	Privacy	Accuracy	Performance	Reliability	Scalability	Interoperability	Time	Cost	Energy
Trust	Manogaran et al. (2018)	*		*	*						
	Gope and Hwang (2016)				*				*		*
	Ullah et al. (2020b)	*			*						*
	Rathee et al. (2019)	*	*	*		*					
	Abou-Nassar et al. (2020)	*	*				*	*			
	Amin et al. (2020)	*		*							

2020b) proposed a fog-assisted HIoT scheme to aggregate and transmit data and provide security against several attacks and illegal data access with low communication cost and energy consumption. Rathee et al. (Rathee et al., 2019) introduced a secure framework about health multimedia data by using blockchain to generate a hash of each data, provide security chains of records, and store them in the network. Therefore, any change in data was reflected in the entire blockchain network, and nobody could perform any illegal activities. Abou-Nassar et al. (Abou-Nassar et al., 2020) proposed a distributed trust framework using blockchain, which provides patients' data privacy, data integrity, and confidentiality, improves HIoT access control and enhances interoperability and security. Finally, Amin, et al. (Amin et al., 2020) used deep learning to design a malware detector to assess the behavior of HIoT applications that detects malwares and improves trust.

5.5.2. A summary of security-based approaches

Monitoring and recommender systems are introduced in application-based approaches to predict and detect anomaly situations or observe the patients for a long time and recommend appropriate medicine to them. The application-based approaches along with significant ideas, the evaluation techniques and tools, and other information, are presented in Table 10. Additionally, Table 11 offers a comparison of some factors such as security, privacy, accuracy.

Privacy, access control, confidentiality, and trust are the main aspects of the security-based methods in the reviewed articles. The main ideas, evaluation techniques, applied tools, and finally, advantages and disadvantages are explained in Table 12. Additionally, a comprehensive comparison of the security-based approaches based on some factors such as security, privacy, accuracy, and performance is presented in Table 13.

6. Analysis of results

Considering the process provided in Section 4, the authors analyze the result of the SLR method in this section. Based on the research question in Section 4.1, we respond to RQ1, RQ2, and RQ3 (shown in Table 2).

6.1. An overview of the primary studies

The following complementary questions are considered to examine the status of research on HIoT:

- What is the state of the research on the HIoT issue?
- What are the councils in which the researchers published their outcomes related to HIoT systems?
- What are the related research communities in HIoT?

Fig. 7 depicts the highest rates of published JCR-indexed journal articles over time. Out of 146 JCR-indexed journal articles until 2020, as illustrated in Fig. 8, 31 % of the articles are related to IEEE, 28 % related to Springer, 27 % to ScienceDirect, 5 % to Wiley, 4 % to SAGE, 2 % to Taylor&Francis, and finally Emerald, Hindawi, and ACM have 1 % of publications each.

As depicted in Table 14, most of the JCR-indexed journal articles on HIoT are published in IEEE IoT-J, IEEE Access, FGCS, IJDSN, COMNET, JOMS, JSUP, and WINET. The JCR-indexed journals that published at least two related articles are listed in Table 14, along with their publisher name, abbreviation, and impact factor.

After selection and synthesis of the papers, the authors' affiliations were extracted. Then, the universities or institutes that published at least two related articles were mentioned as active research communities. Table 15 shows the list of research communities and their research focuses. Additionally, a significant number of research papers on HIoT were published by researchers from Islamic Azad University in Iran, the University of California in the USA, Guru Nanak Dev University in India, National Institute of Technology Patna in India, Sikkim University in

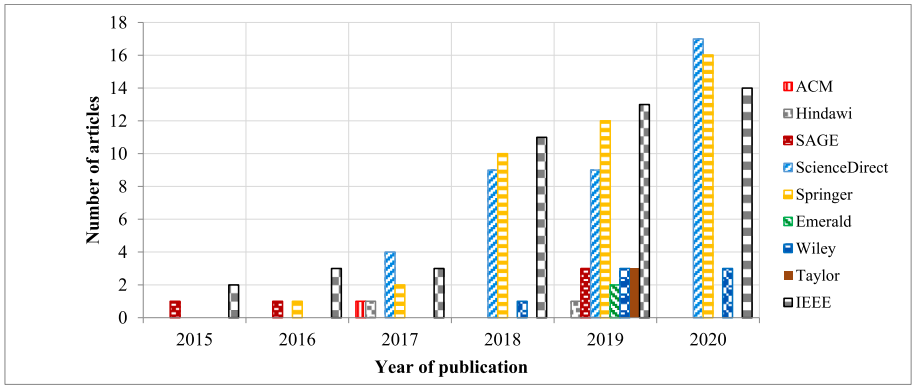

Fig. 7. The distribution of JCR-indexed journal articles over time in each investigated publisher.

India, and SASTRA University in India.

6.2. Research objectives, techniques, and evaluation parameters

This subsection aims to respond to the RQs mentioned in Section 4.1, based on a statistical analysis of the reviewed approaches.

➢ RQ2: What research scopes exist in IoT-based healthcare systems? Besides, what achievements are there in this area?

As a quantitative answer to this question, based on Fig. 9, the highest percentage of IoT-based healthcare approaches is related to the security-based category with 54 research studies or nearly 37 % of 146 articles. In this category, investigations are most related to privacy, access control, confidentiality, and trust. The next category of approaches is related to application-based approaches with 32 % of all studied papers, including monitoring and recommender systems. The third group of high frequent articles is related to the sensor-based group with 12 % of all studied papers, including wearable and environmental sensors. The fourth is related to resource-based approaches with 10 % of all studied papers, including scheduling, resource allocation, offloading, load balancing, and provisioning methods. With 9 % of all studied papers, the last one is related to communication-based approaches, including technological and algorithmic approaches. In addition, as a qualitative answer, the merits and demerits of the classified approaches are presented in Table 16.

➢ RQ3: What are the existing techniques and methods to enable IoT in healthcare systems?

To answer this question, the authors evaluate HIoT systems in three dimensions, including evaluation factors, evaluation techniques, and evaluation tools as follows.

- Evaluation factors

According to Tables 5, 7, 9, 11 and 13, performance (22 %), security (21 %), and time (18 %), respectively, are the essential metrics among all applied factors, as shown in Fig. 10. In the sensor-based approaches, as illustrated in Fig. 11, performance (27 %), energy (24 %), and reliability (13 %) are the most applied metrics. In the resource-based group, such parameters as time (41 %), energy (17 %), and reliability (10 %) have attracted researchers' attention more than other parameters. Authors have attempted to improve time by 27 % and performance and energy with 21 % in the communication-based category. The performance and accuracy with 22 % and time with 19 % are other important parameters in the application-based approaches. In security-based approaches, such parameters as privacy, access control, confidentiality, and trust with 40 %, performance with 21 %, and time with 14 % are important parameters. It should be noted that the mentioned percentages have obtained from (1) (Hamzei and Navimipour, 2018):

$$Percentage\ P(i) = \frac{\text{Frequency\_ P(i)}}{\sum_{j=1}^{\text{number of P}} \text{Frequency\_ P(j)}} \times 100 \quad (1)$$

To obtain the percentage of Parameter (i), the frequency of Parameter (i) was counted and divided by the sum of parameters frequencies, then 100 is multiplied by the calculated value.

- Evaluation techniques

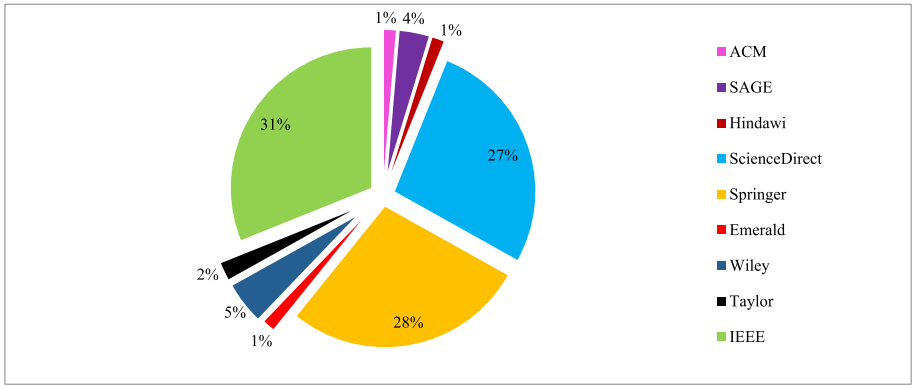

Fig. 8. A pie chart of the percentage of JCR-indexed journal articles based on different publishers.

Table 14
Papers distribution per publication channel.

Publisher	Publication channel	Abbreviation	Count	Impact factor (2020)
Elsevier	Future Generation Computer Systems	FGCS	11	7.187
	Computer Networks	COMNET	7	4.474
	Information Sciences	InfSci	3	6.795
	Computers & Electrical Engineering	CEE	2	3.818
	Computer Communications	COMCOM	2	3.167
	Sustainable cities and society	SCS	2	7.587
	Measurement	MEAS	2	3.927
	Sustainable Computing	SUSCOM	2	4.028
Hindawi	Wireless Communications and Mobile Computing	WCMC	2	2.336
IEEE	IEEE Access	IEEE Access	14	3.367
	IEEE Internet of things journal	IEEE IoT-J	14	9.471
	IEEE Systems Journal	ISJ	3	3.931
	IEEE Sensors Journal	IEEE SensJ	2	3.301
	IEEE Transactions on Circuits and Systems I: Regular Papers	IEEE CAS	2	3.605
	IEEE Transactions on Industrial Informatics	IEEE TII	2	10.215
SAGE	International Journal of Distributed Sensor Networks	IJDSN	4	1.640
Springer	Ambient Intelligence and Humanized Computing	JAIHC	8	7.104
	Journal of Medical Systems	JOMS	5	4.460
	Journal of Supercomputing	JSUP	4	2.474
	Wireless Networks	WINET	4	2.602
	Peer-to-Peer Networking and Applications	PPNA	3	3.307
	Multimedia Tools and Applications	MTAP	3	2.757
	Cluster Computing	CLUS	3	1.809
	Mobile Networks and Applications	MNA	2	3.426
	Neural Computing and Applications	NCAA	2	5.606
Taylor	IETE Journal of Research	TIJR	3	2.333
Wiley	Transactions on Emerging Telecommunications Technologies	ETT	3	2.638
	Concurrency and Computation: Practice and Experience	CPE	2	1.536
	International Journal of Communication Systems	IJCS	2	2.047

According to Tables 4, 6, 8, 10 and 12, simulation, real testbed, prototype, formal, and design are the evaluation techniques applied in the studied articles. According to Fig. 12, simulation has been used more than other techniques with 57 % then real testbed with 24 %, and prototype and formal have been used with 10 % each.

- Evaluation tools and environments

To achieve correct and efficient design before a system is constructed, some popular simulation and modeling tools are used by developers. In this regard, based on Tables 4, 6, 8, 10 and 12, the common tools and environments used in the selected articles are MATLAB, C/C++/C#, Python, Weka, NS2/NS2, and so on. In addition, the popularity of MATLAB and C/C++/C# is more than other applied tools and environments, as shown in Fig. 13.

Table 15
Active communities and their research focus.

University/Institute	Studies	Research Focus
Islamic Azad University, Iran	(Esmaeili et al., 2020), (Akhbarifar et al., 2020), (Hosseinzadehet al., 2020b), (Rahmani et al., 2020), (Ghasemi et al., 2019), (Asghari et al., 2019b)	Application-based and sensor-based approaches
University of California, USA	(Azimi et al., 2019), (Muthuet al., 2020), (Azimiet al., 2017), (Subramaniyaswamyet al., 2018), (Rahmaniet al., 2018)	Sensor-based and application-based approaches
Guru Nanak Dev University, India	(Bhatia and Sood, 2017), (Verma and Sood, 2018), (Sood and Mahajan, 2019), (Verma et al., 2018), (Sharma and Kalra, 2019)	Sensor-based, application-based, and security-based approaches
National Institute of Technology Patna, India	(Ray et al., 2019a), (Ray et al., 2019c), (Ray et al., 2019d), (Ray et al., 2018), (Ray et al., 2019e)	Resource-based, sensor-based, application-based, and communication-based approaches
Sikkim University, India	(Ray et al., 2019a), (Ray et al., 2019c), (Ray et al., 2019d), (Ray et al., 2018), (Ray et al., 2019e)	Resource-based, sensor-based, application-based, and communication-based approaches
SASTRA University, India	(Manikandan et al., 2020), (Patan et al., 2020), (Subramaniyaswamyet al., 2018), (Rani et al., 2019), (Elhoseny et al., 2018)	Security-based, application-based, communication-based and resource-based approaches
Thapar Institute of Engineering and Technology, India	(Kaur et al., 2019), (Ray et al., 2019e), (Sharma et al., 2020), (Sun et al., 2020)	Application-based, communication-based, and security-based approaches
Maulana Abul Kalam Azad University of Technology, India	(Ray et al., 2019a), (Ray et al., 2019c), (Ray et al., 2019d), (Ray et al., 2018)	Resource-based, sensor-based, and application-based approaches
University of Florida, USA	(Huang et al., 2019), (Karimian et al., 2019), (Zhou and Piramuthu, 2018), (Jia et al., 2018)	Security-based approaches
Bahria University, Pakistan	(Jabbar et al., 2017), (Ullah et al., 2017), (Awanet al., 2019)	Application-based and resource-based approaches
Institute of Computer Technology, Austria	(Azimi et al., 2019), (Azimiet al., 2017), (Rahmaniet al., 2018)	Sensor-based, and application-based approaches
Sejong University, South Korea	(Aliet al., 2018), (Hamza et al., 2020), (Kaw et al., 2019)	Application-based, and security-based approaches
Sri Ramanujar Engineering College, India	(Kumar et al., 2018), (Suresh et al., 2019), (Manogaran et al., 2018)	Application-based, and security-based approaches
Sungkyul University, South Korea	(Elmisery et al., 2016), (Elmisery et al., 2017), (Li et al., 2018)	Security-based approaches
Universidad Tecnica Federico Santa Maria, Chile	(Elmisery et al., 2016), (Elmisery et al., 2017), (Li et al., 2018)	Security-based approaches
University of Turku, Finland	(Azimi et al., 2019), (Azimiet al., 2017), (Rahmaniet al., 2018)	Sensor-based and application-based approaches
VIT University, India	(Kumar et al., 2018), (Kumar and Gandhi, 2017), (Manogaran et al., 2018)	Application-based and security-based approaches
King Saud University, KSA	(Vilela et al., 2019), (Fouad et al., 2020), (Alhussein et al., 2018)	Sensor-based and application-based approaches
Duy Tan University, Vietnam	(Akhbarifar et al., 2020), (Hosseinzadehet al., 2020b), (Rahmani et al., 2020)	Application-based approaches

(continued on next page)

Table 15 (*continued*)

University/Institute	Studies	Research Focus
Arab Academy for Science, Technology, and Maritime Transport, Egypt	(Elmisery et al., 2017), (Li et al., 2018)	Security-based approaches
Beijing University of Posts & Telecommunications, China	(Yang et al., 2016), (He et al., 2017)	Sensor-based and resource-based approaches
Central South University, China	(Chen et al., 2018), (Tang et al., 2019)	Sensor-based and security-based approaches
COMSATS Institute of Information Technology, Pakistan	(Jabbar et al., 2017), (Ullah et al., 2017)	Application-based approaches
ESCP Business School, France	(Zhou and Piramuthu, 2018), (Jia et al., 2018)	Security-based approaches
Indian Institute of Technology, India	(Tuliet al., 2020), (Kavitha and Sharma, 2019)	Application-based and resource-based approaches
SRM Valliammai Engineering College, India	(Kesavan and Arumugam, 2020), (Kavitha and Ravikumar, 2020)	Application-based approaches
Khalifa University of Science and Technology, UAE	(Tekeste et al., 2019), (Hallforset al., 2018)	Sensor-based approaches
Iran University of Medical Sciences, Iran	(Akhbarifar et al., 2020), (Hosseinzadehet al., 2020b)	Application-based approaches
Macquarie University, Australia	(Pal et al., 2019), (Yang et al., 2019)	Security-based approaches
Monash University, Australia	(Wu et al., 2017), (Wu et al., 2018)	Sensor-based approaches
National Dong Hwa University, Taiwan	(Yeh, 2016), (Hou and Yeh, 2015)	Security-based approaches
National Institute of Standards and Technology, USA	(Laplante et al., 2018), (Laplante et al., 2018)	Application-based approaches
Pennsylvania State University, USA	(Laplante et al., 2018), (Laplante et al., 2018)	Application-based approaches
Singapore Approaches University, Singapore	(Yang et al., 2018), (Xu et al., 2019)	Security-based approaches
King Fahd University, KSA	(Abuelkhail et al., 2020), (AbdulGhaffar et al., 2020)	Application-based and communication-based approach
University of Newcastle, Australia	(Pal et al., 2019), (Yang et al., 2019)	Security-based approaches
University of Regina, Canada	(Onasanya and Elshakankiri, 2019), (Onasanya et al., 2019)	Application-based approaches
Wayne State University, USA	(Tekeste et al., 2019), (Hallforset al., 2018)	Sensor-based approaches
Widener University, USA	(Laplante et al., 2018), (Laplante et al., 2018)	Application-based approaches
Shahed University, Iran	(Akhbarifar et al., 2020), (Fotouhi et al., 2020)	Application-based and security-based approach
Anna University, India	(Muthuet al., 2020), (Sharavana Kumar and Sarma Dhulipala, 2020)	Sensor-based and communication-based approach
Velagapudi Ramakrishna Siddhartha Engineering College, India	(Manikandan et al., 2020), (Patan et al., 2020)	Communication-based and resource-based approaches
Maharaja Agrasen Institute of Technology, India	(Bharathiet al., 2020), (Patan et al., 2020)	Communication-based and resource-based approaches
National University of Singapore, Singapore	(Sengupta and Bhunia, 2020), (Gope et al., 2020)	Application-based and resource-based approaches
Beirut Arab University, Lebanon	(Muthuet al., 2020), (Huifeng et al., 2020)	Sensor-based approaches

7. Open issues, future trends, and challenges

Now, there exist significant problems to improve IoT-based healthcare systems that have not been studied much in the current research trends. In this section, to answer RQ4, open issues, future trends, and challenges in HIoT systems have been debated.

➢ RQ4: What are the key open issues, future trends, and challenges in IoT-based healthcare systems?

After analyzing the collected data through this review on the HIoT field and also regarding the increasing requirements for applying effective HIoT systems in the real physical world, we observed that open issues, challenges, and future directions can be categorized into three separate groups as shown in Fig. 14.

The main challenges that HIoT systems involve are scalability, interoperability, and mobility. Furthermore, the lack of a real testbed environment for evaluating the efficiency of HIoT systems in the real world can be considered as another important challenge in developing HIoT systems. On the other hand, regarding the mentioned challenges, several issues have remained as open issues to be addressed: the relevant problems of computing environments like fog computing in which the HIoT system is developed and deployed, and some operational and technical problems like power and resource management issues regarding the limitation of storage and computing capacity of fog nodes. According to different expected objectives in HIoT systems, other open issues comprise multi-objective optimization and providing privacy and trust. With respect to the increasing need to apply computer-aided technologies in developing healthcare systems, some directions in the HIoT field, including IoNT, Blockchain, Tactile Internet, SDN/NFV, online social networks, big data analysis, and QoS, can be considered as future trends. Details of the mentioned challenges, open issues, and future trends are explained in the following section.

7.1. Open issues

- Trust and privacy: In the reviewed literature, trust, and privacy management (Boussada et al., 2019), (Elmisery et al., 2016), (Saha et al., 2019), (Tao et al., 2019), (Jiang et al., 2019), (Tang et al., 2019), (Baek et al., 2016), (Elmisery et al., 2017), (Li et al., 2018), (Rani et al., 2019), (Hamza et al., 2020), (Guo et al., 2020), (Manogaran et al., 2018), (Gope and Hwang, 2016), (Ullah et al., 2020b), (Rathee et al., 2019), (Abou-Nassar et al., 2020), (Amin et al., 2020) are significant open issues for data access and data storage in IoT-based healthcare platforms. Trust can be defined as managing credentials and controlling access to service providers' and patients' confidential information and privacy as preventing unauthorized access to both of them. Healthcare IoT-based systems are designed and expanded based on the obtained data from IoT devices. Furthermore, with the increase in the number of IoT devices connected to the network, the vulnerability of the immense data being transferred and stored is also increased (Boussada et al., 2019), (Manogaran et al., 2018). Nonetheless, according to the reviewed studies, a few papers have adequately evaluated this critical metric. Therefore, to reduce the risk of hacking essential data and to increase data protection such as a person's behavior pattern, habits, sleeping order, locations, and physical conditions over time-trust and privacy are very challenging as open issues.
- Power management: Based on the studied literature, energy consumption (Wu et al., 2017), (Wu et al., 2018), (Niitsuet al., 2018), (Tekeste et al., 2019), (Hallforset al., 2018), (Ray et al., 2019d),

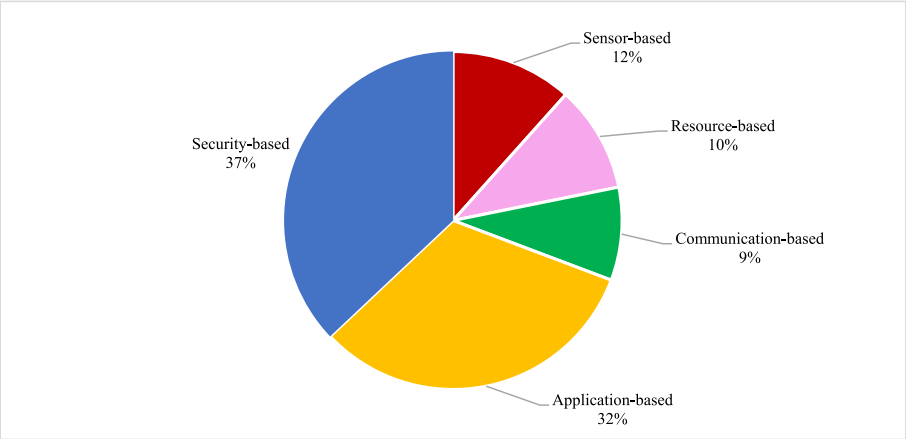

Fig. 9. The percentage of IoT-based healthcare approaches.

Table 16
Merits and demerits of the classification approaches.

	Sensor-based	Resource-based	Communication-based	Application-based	Security-based
Merits	➢ Better performance ➢ Better reliability ➢ Better energy ➢ Better cost	➢ Better optimization ➢ Better performance ➢ Better reliability ➢ Better latency ➢ Better energy	➢ Better performance ➢ Better reliability ➢ Better latency ➢ Better energy ➢ Better overhead	➢ Better performance ➢ Better flexibility ➢ Better accuracy ➢ Better latency	➢ Better privacy ➢ Better access control ➢ Better confidentiality ➢ Better trust ➢ Better performance ➢ Better accuracy ➢ Better latency
Demerits	➢Unsatisfied security & privacy ➢Unsatisfied scalability	➢Unsatisfied security & privacy ➢Unsatisfied scalability	➢ Unsatisfied security & privacy ➢ Unsatisfied scalability ➢ Unsatisfied cost	➢ Unsatisfied security & privacy ➢ Unsatisfied scalability ➢ Unsatisfied energy ➢ Unsatisfied cost ➢ Unsatisfied interoperability	➢ Unsatisfied scalability ➢ Unsatisfied cost ➢ Unsatisfied interoperability

(Elstset al., 2018), (Chen et al., 2018), (Abdelmoneem et al., 2020), (Awanet al., 2019), (Sengupta and Bhunia, 2020), (Minet al., 2019), (Bharathiet al., 2020), (Catarinucciet al., 2015), (Abdellatif et al., 2018), (Aktas et al., 2018), (Chehri and Mouftah, 2020), (Qiu et al., 2017), (Chanak and Banerjee, 2020), (Sharavana Kumar and Sarma Dhulipala, 2020), (Tuliet al., 2020), (Rahmaniet al., 2018), (Ramírez López et al., 2019), (Onasanya et al., 2019), (Vedaeiet al., 2020), (Boussada et al., 2019), (Tao et al., 2019), (Rani et al., 2019), (Hamza et al., 2020), (Yang et al., 2019), (Aghili et al., 2019), (Karimian et al., 2019), (Benadda et al., 2018), (Gupta et al., 2020), (Xu, 2020), (Islam and Young Shin, 2020), (Li and Jing, 2019), (Gope and Hwang, 2016), (Ullah et al., 2020b) is the main open issue to decrease high operational costs and massive carbon production in HIoT systems. In addition, a typical HIoT network includes small devices with limited battery power. Therefore, some factors, such as systematic standby control and data migration, have important roles in achieving inferior energy consumption without decreasing the quality of smart healthcare services (Chen et al., 2018). Hence, low

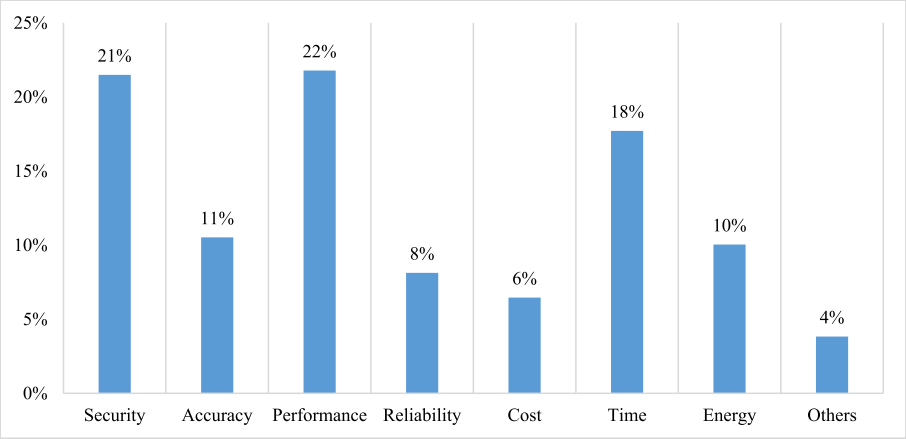

Fig. 10. The percentage of evaluation factors in all investigations.

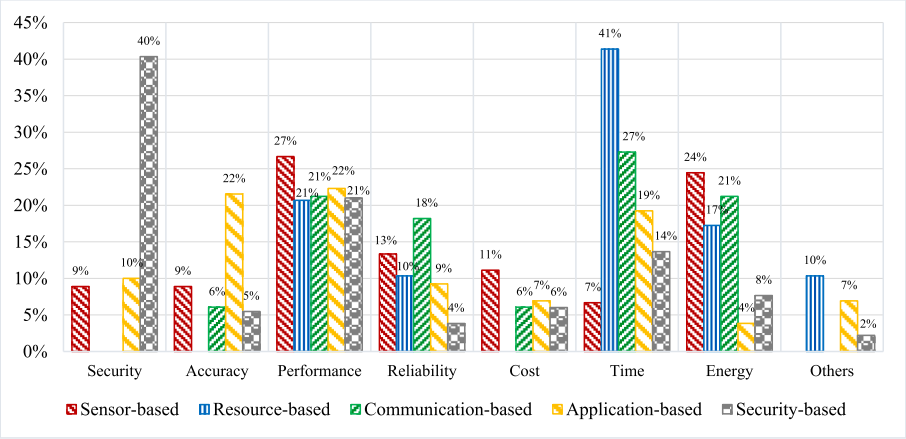

Fig. 11. The percentage of evaluation factors in each category.

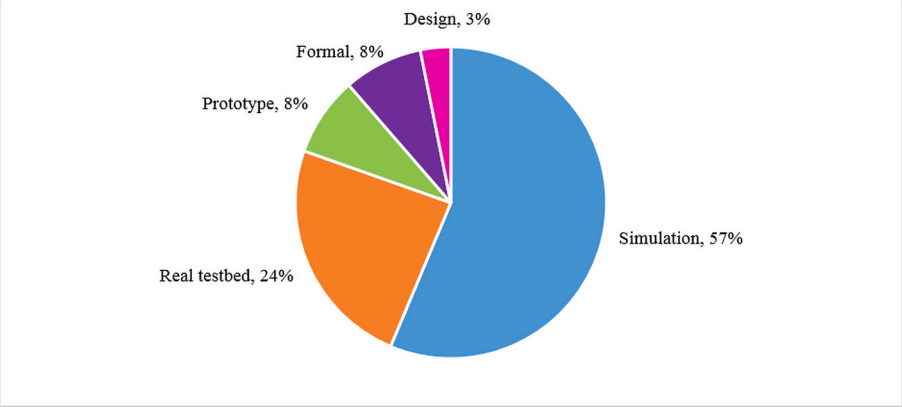

Fig. 12. The percentage of evaluation techniques in all investigations.

power devices have to be designed to increase HIoT systems' lifetime and decrease the possibility of patients being offline. Therefore, another challenge of HIoT is power management.

- Fog computing: Fog computing (Abdelmoneem et al., 2020), (Asif-Ur-Rahmanet al., 2019), (Awaisi et al., 2020), (Wang and Li, 2020), (He et al., 2017), (Ray et al., 2019e), (Sood and Mahajan, 2019), (Azimiet al., 2017), (Tuliet al., 2020), (Rajan et al., 2020), (Kesavan and Arumugam, 2020), (Rahmaniet al., 2018), (Elmisery et al., 2016), (Saha et al., 2019), (Jia et al., 2018), (Sun et al., 2020), (Li and Jing, 2019), (Ullah et al., 2020a) is crucial in healthcare IoT

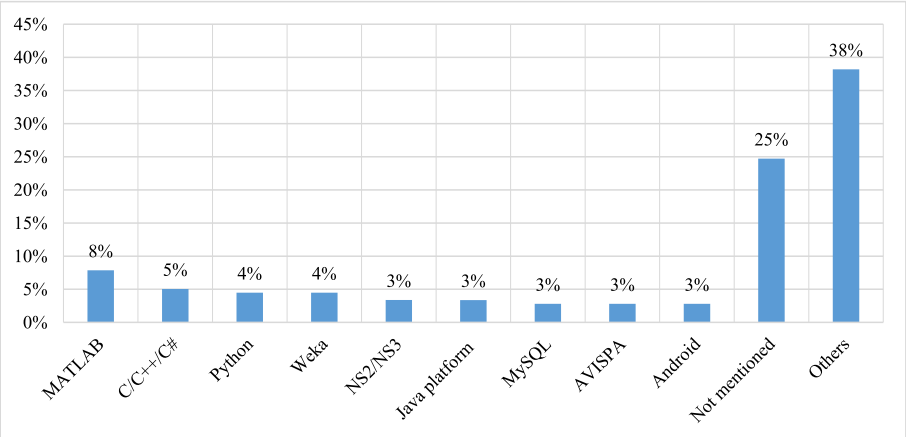

Fig. 13. The percentage of trending evaluation tools in the selected articles.

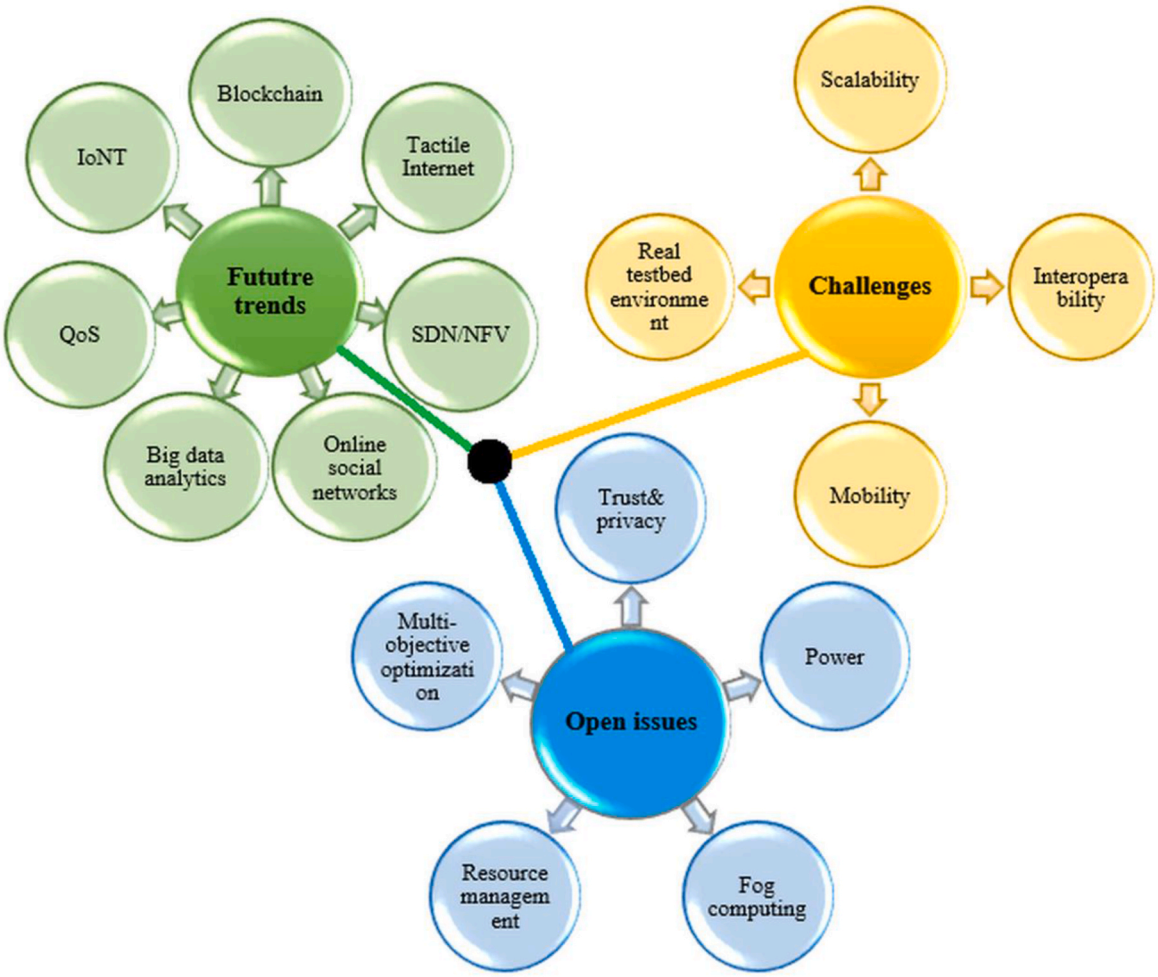

Fig. 14. An overview of open issues, future trends, and challenges in HIoT.

environments as the location of computing is dynamic and depends on requirements of the environment, contexts, and applications. Additionally, it needs low and predictable latency to provide service delivery to end-users in emergencies, to minimize the volume of transferred data to the cloud while vital data are being transferred to the fog for processing and storage, and to reduce bandwidth and battery resources. Despite many advances in this area, more activities are needed to satisfy the mentioned requirements in HIoT systems (Rajan et al., 2020), (Rahmaniet al., 2018). Therefore, fog computing is very challenging for researchers.

- Resource management: HIoT nodes have limited computational power and storage; their assignments are tremendous. Therefore, managing and efficiently using smart healthcare devices is critical in the HIoT environment. Generally, the resource management (Ray et al., 2019a), (Abdelmoneem et al., 2020), (Yi and Cai, 2019), (Awanet al., 2019), (Manikandan et al., 2020), (Asif-Ur-Rahmanet al., 2019), (Kavitha and Sharma, 2019), (Sengupta and Bhunia, 2020), (Awaisi et al., 2020), (Minet al., 2019), (Wang and Cai, 2020), (He et al., 2017), (Bharathiet al., 2020), (Kumar and Silambarasan, 2019) can lead to more studies and investigations. Additionally, with the mobility and relocation properties of smart devices, resource management should efficiently apply various services to create an optimal application of the accessible resources and provide appropriate services in HIoT (Asif-Ur-Rahmanet al., 2019). Therefore, another important open issue of this study is resource management.
- Multi-objective optimization: In the reviewed literature, it is clear that some QoS factors of HIoT systems were considered, and the others were ignored. For example, in some algorithms, cost and delay are considered, and other factors like reliability and power, are ignored. Therefore, an optimal mechanism that considers different objectives to create a tradeoff among different QoS factors in HIoT systems (Niitsuet al., 2018), (Esmaeili et al., 2020), (Ray et al., 2019d), (Elstset al., 2018), (Chen et al., 2018), (Sengupta and Bhunia, 2020), (Minet al., 2019), (Catherwood et al., 2018), (Aktas et al., 2018), (Qiu et al., 2017), (Ray et al., 2019e), (Sharavana Kumar and Sarma Dhulipala, 2020), (Patan et al., 2020), (Vedaraj and Ezhumalai, 2020), (Azimiet al., 2017), (Khowaja et al., 2018), (Tuliet al., 2020), (Alhussein et al., 2018), (Rajan et al., 2020), (Ray et al., 2018), (Rahmani et al., 2020), (Kesavan and Arumugam, 2020), (Ramírez López et al., 2019), (Ghasemi et al., 2019), (Vedaeiet al., 2020), (Lin et al., 2019), (Asghari et al., 2019b), (Boussada et al., 2019), (Tao et al., 2019), (Rani et al., 2019), (Hamza et al., 2020), (Karimian et al., 2019), (Vaishnavi and Sethukarasi, 2020), (Sun et al., 2020), (Gupta et al., 2020), (Sun et al., 2020), (Li and Jing, 2019), (Ming et al., 2020), (Ullah et al., 2020a), (Gope and Hwang, 2016) may be an open issue.

7.2. Future trends

- *Blockchain*: Another option that could be associated with the future of the edge/IoT environment is blockchain. The incapability to

change information or delete from blocks makes the blockchain the best appropriate technology for the healthcare system by providing secure management and analysis of big health data. Moreover, it is an immutable, clear consensus and permanent protocol to leverage peer-to-peer and distributed communication without the need for centralized authority; the "Internet of edge-block" may be supposed to help the existing edge-IoT environment to act transparently and autonomously while processing the decentralized end-users' requests (Qadri et al., 2020), (Rathee et al., 2019), (Ali et al., 2019). Indeed, this problem has not received much attention from the researchers, so, to this end, blockchain in HIoT can be an interesting direction for the future.

- Tactile Internet: The idea of Internet sensorial connectivity is called tactile Internet (TI). It is based on IEEE's definition of communication standardization among devices to reproduce the stimuli and senses and create perception capability in the digital world. The emergence of 5G communication technology led to probing TI-based applications in healthcare and robotics fields specifically. The role of TI in healthcare can be applied at tremor suppression in Parkinson's disease, remote surgeries, interactive medical training, trauma rehabilitation, virtual and augmented reality-based training and rehabilitation, and so on (Ruan et al., 2017). Therefore, TI applications have some potentials in HIoT that can be good opportunities for future research.
- SDN/NFV: Regarding the limitation of HIoT resources, software-defined network (SDN) support in HIoT systems can make the management of HIoT more proper. The mixture of HIoT and network function virtualization (NFV) provide speed and flexibility in the construction, management, and deployment of novel applicant-based services (Sun et al., 2020), (Hu et al., 2015). Using SDN and NFV technologies to support QoS needs in HIoT is an engrossing area for future research.
- Online social networks: Online social networks might act as a trustworthy online platform to found interfaces of service application among healthcare providers (HP) and healthcare users (HU) anytime and anywhere. This paradigm enables the IoT medical devices to HU's bio-data with remote HP through both computational resource-rich and storage-rich social networks. The nodes of social networks are friendship, work, common interests, knowledge, prestige, etc., that can be organized to exchange information, knowledge, or financial assistance (Hao and Wang, 2017), (Bazzaz Abkenar et al., 2021). This paradigm in HIoT is a new area to predict the patient's health status, and it has excellent potentials for future studies.
- Big data analytics: IoT big data analytics have been the base of recent smart healthcare systems. In other words, the convergence of big data analytics and IoT has ended in the development of modern medical telematics and informatics such as diagnosis of diseases, remote and real-time health monitoring systems, prevention systems, and medical emergency and alerting systems (Saheb and Izadi, 2019). The data obtained from heterogeneous devices in IoT environments have an extended volume of information related to users' personal lifestyles in the long run and have the various, complicated, and complete context of other information related to health. It is significant to study the manner of exploring all these big data under IoT systems to bring intelligence for policy formulation and more decisive clinical decision-making, but this issue has not received much attention in all investigations (Qi et al., 2017), (Yang et al., 2019), (Manogaran et al., 2018), (Fathi et al., 2021). Hence, big data analytics in IoT-based healthcare systems is another interesting line for future studies.
- Service quality: Recently, HIoT has been applied for real-time applications. QoS mostly deals with the quality and timeliness of the HIoT data used to support the decision. It is required that the data produced from sensors of healthcare be collected, analyzed, transferred, and applied on time; however, sometimes, the necessary data are not provided immediately, which seems to be a challenge for HIoT systems. IoT devices produce wide-scale real-time data in terms of variety, volume, and velocity, leading to a considerable challenge in analyzing such data. As medical wearable systems deal with real-time and life-critical applications, they need a strong guarantee of QoS. There is a wide gap in different areas like real-time tracking of patients, data collection, and automated decision-making support based on QoS (Dhanvijay and Patil, 2019), (Patan et al., 2020), (Ray et al., 2018). No need to say that these challenges have to be overcome on the basis of QoS.
- Internet of nano things: With the emergence of the Internet of nano things (IoNT), numerous applications can be recognized by IoNT for healthcare, including nanorobots for delivering drugs to special organs with great accuracy, nanosensors, precision medicine, minimally invasive surgical procedures, and a swarm of nanorobots for human body parts that are not accessible (Pramanik et al., 2020). Finally, the IoNT is leading the network revolution at the nanoscale with applications in sensing and precision medicine as a future direction.

7.3. Challenges

- Scalability: Another significant criterion in the healthcare system is scalability. In other words, it is the ability of a system to satisfy the changing needs and adapt to the changes on a bigger scale in the future. In the literature studied, some of the proposed approaches in HIoT systems can operate on a small scale, and the validity of these approaches is just guaranteed by some nodes or devices. Scalability is an important factor. However, the suggested approaches were mostly used in limited scenarios, which seems to be a challenge.
- Interoperability and standardization: Interoperability is a major factor in exchanging resources and data between patients and smart objects in HIoT. Interoperability's main challenge is developing open-source frameworks with a steady connection; a collection of standards has to be set to make horizontal platforms capable of operability, programmability, and communicability among devices, operating systems, and applications, not having any concerns about the manufacturer or the model. Having some architectures that are scalable to interact with non-homogeneous data centers and smart objects and procuring dynamic and adaptive architectures that are interoperable for large-scale IoT applications are other challenges (Jabbar et al., 2017). Totally, the open challenge in HIoT systems is interoperability and standardization.
- Mobility: Mobility is one of the major challenges in HIoT, which has been less discussed in the literature. Mobility in IoT healthcare systems is the ability to use network support for the patients that can connect to the gateway anytime and anywhere. Further, mobility is necessary to make the network fault-tolerant, provides complete access to information disregarding their locations, and enhance service quality. Due to the importance of provisioning in healthcare, a mobility protocol must be reliable to decrease packet losses, network failures under any circumstances, and end-to-end delays because (Rahmaniet al., 2018). Therefore, mobility is an interesting challenge for research.
- Real testbed environment: The HIoT approaches proposed in the studies should be implemented in real environments, while only 24 % of the reviewed studies have been conducted in real testbeds (as shown in Fig. 12), and the others have been tested with simulation tools. Frankly speaking, all the proposed approaches must be implemented in real testbeds to conclude whether they can provide a suitable healthcare system or not. Therefore, real testbed implementation is a challenge.

8. Threats to validity and limitations

Threats to the validity of this research study are considered in several steps as follows:

Step 1. Threats to the identification of complete primary articles: In the research strategy, the most crucial factor is to collect comprehensive available literature without any bias. To this end, the common strings were searched and combined in the search term. Besides, a review protocol was designed to identify relevant and unbiased studies.

Step 2. Threats to selection and data extraction: In systematic reviews, each study deals with a quality assessment (Brereton et al., 2007):

- *The bias in the result*: The aim is to have the correct results.
- *Internal validity*: The goal is to conduct the study without systematic error.
- *External validity*: The aim is to see the applicable effects outside the context of the study.

Two types of quality assessments are used in this investigation. The first type was to assess the articles' quality with their ability to answer the research questions, and the second kind was applied to respond to one of our primary RQs.

Step 3. Threats to data synthesizes and results: The reliability threat is another challenge of reviews (Jamshidi et al., 2013). This issue was obtained from a unified characterization model, multiple researchers, and several other steps in which method and process were piloted and externally evaluated. Although we used the guidelines in (Brereton et al., 2007), (KitchenhamKeele, 2004) to provide an SLR, we had deviations from their methods described in Section 4.

With the use of a systematic review, external evaluations, and different researchers, we can claim that the validity of the review is high.

This review aimed at providing a comprehensive and systematic review; however, some limitations of this study should be considered in the future as follows:

- In this research, only reputed journal articles are regarded for their best qualifications. Therefore, books, book chapters, conference papers, symposiums, non-English scripts, non-JCR papers, commentaries and review articles, and short articles have been excluded.
- Due to the wide range of literature on the topic of HIoT systems, only JCR-indexed journal articles were considered despite other reputed conference articles.
- In this manuscript, we applied ten-known online databases that suggested relevant reputed papers. However, the authors cannot claim to have selected all articles on the HIoT subject.
- In Section 4.1, four questions were asked to expand this topic; however, other problems can be proposed.
- The reviewed articles in this research were categorized into five classes, including sensor-based, resource-based, communication-based, application-based, and security-based approaches. However, other classes might be possible.

9. Conclusion

This paper presented an SLR on the Internet of things in healthcare systems. First, 1343 articles between 2015 and 2020 were selected; then, based on the inclusion/exclusion criteria, 146 articles out of 1343 articles were selected to analyze and exploit appropriate data. With respect to RQ2, the selected articles were classified into five classifications, including sensor-based, resource-based, communication-based, application-based, and security-based approaches. According to our classifications, the security-based category was on the top of others with 37 % frequency, while the application-based by 32 %, the sensor-based by 12 %, the resource-based by 10 %, and the communication-based by 9 % came next respectively. Further, the main idea of each paper, along with its benefits and limitations, were explored. In addition, based on RQ3, the evaluation factors, types, and used tools in the studied articles were discussed. According to the statistics, most articles attempted to improve the performance by 22 %, security by 21 %, and time by 18 %. Moreover, the comparison of evaluation techniques indicated that 57 % of the studied articles employed simulation environments, and 24 % employed real testbeds to evaluate HIoT systems. Besides, MATLAB and C/C++/C# are the applied evaluation tools and environments. Eventually, according to RQ4, to develop more efficient HIoT systems, some open issues and future trends such as power management, trust and privacy, fog computing, multi-objective optimization, resource management, QoS, blockchain, tactile Internet, SDN/NFV, online social networks, big data analytics, and IoNT should be considered. Lucidly, the most important challenges are interoperability, scalability, mobility, and real-testbed implementation. We assuredly hope that these results will help other researchers to develop HIoT systems efficiently as their future works.

Declaration of competing interest

The authors report no conflicts of interest. The authors alone are responsible for the content and writing of this article.

References

Abdellatif, A.A., Khafagy, M.G., Mohamed, A., Chiasserini, C., 2018. EEG-based transceiver design with data decomposition for healthcare IoT applications. IEEE Internet of Things Journal 5 (5), 3569–3579.

Abdelmoneem, R.M., Benslimane, A., Shaaban, E., 2020. Mobility-aware task scheduling in cloud-Fog IoT-based healthcare architectures. Comput. Network. 179, 107348–107365.

AbdulGhaffar, A., Mostafa, S.M., Alsaleh, A., Sheltami, T., Shakshuki, E.M., 2020. Internet of Things based multiple disease monitoring and health improvement system. Journal of Ambient Intelligence and Humanized Computing 11 (3), 1021–1029.

Abou-Nassar, E.M., Iliyasu, A.M., El-Kafrawy, P.M., Song, O., Bashir, A.K., El-Latif, A.A. A., 2020. DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems. IEEE Access 8, 111223–111238.

Abuelkhail, A., Baroudi, U., Raad, M., Sheltami, T., 2020. Internet of things for healthcare monitoring applications based on RFID clustering scheme. Wireless Network 27 (1), 747–763.

Aghili, S.F., Mala, H., Shojafar, M., Peris-Lopez, P., 2019. LACO: lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. Future Generat. Comput. Syst. 96, 410–424.

Ahmadi, H., Arji, G., Shahmoradi, L., Safdari, R., Nilashi, M., Alizadeh, M., 2018. The application of internet of things in healthcare: a systematic literature review and classification. Univers. Access Inf. Soc. 18 (4), 837–869.

Ahmadi, Z., Haghi Kashani, M., Nikravan, M., Mahdipour, E., 2021. Fog-based healthcare systems: A systematic review. Multimedia Tools Appl. In press.

Ahmed, A., Latif, R., Latif, S., Abbas, H., Khan, F.A., 2018. Malicious insiders attack in IoT based multi-cloud e-healthcare environment: a systematic literature review. Multimed. Tool. Appl. 77 (17), 21947–21965.

Akhbarifar, S., Javadi, H.H.S., Rahmani, A.M., Hosseinzadeh, M., 2020. A secure remote health monitoring model for early disease diagnosis in cloud-based IoT environment. Personal Ubiquitous Comput. 24 (6), 815–832.

Aktas, F., Ceken, C., Erdemli, Y.E., 2018. IoT-based healthcare framework for biomedical applications. J. Med. Biol. Eng. 38 (6), 966–979.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M., 2015. Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials 17 (4), 2347–2376.

Al-Turjman, F., Alturjman, S., 2018. Context-sensitive access in industrial internet of things (IIoT) healthcare applications. IEEE Transactions on Industrial Informatics 14 (6), 2736–2744.

Alam, M.M., Malik, H., Khan, M.I., Pardy, T., Kuusik, A., Le Moullec, Y., 2018. A survey on the roles of communication technologies in IoT-based personalized healthcare applications. IEEE Access 6, 36611–36631.

Alam, M.G.R., Abedin, S.F., Moon, S.I., Talukder, A., Hong, C.S., 2019. Healthcare IoT-based affective state mining using a deep convolutional neural network. IEEE Access 7, 75189–75202.

Alhussein, M., Muhammad, G., Hossain, M.S., Amin, S.U., 2018. Cognitive IoT-cloud integration for smart healthcare: case study for epileptic seizure detection and monitoring. Mobile Network. Appl. 23 (6), 1624–1635.

Ali, M.S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., Rehmani, M.H., 2019. Applications of blockchains in the internet of things: a comprehensive survey. IEEE Communications Surveys & Tutorials 21 (2), 1676–1717.

Ali, F., et al., 2018. Type-2 fuzzy ontology–aided recommendation systems for IoT–based healthcare. Comput. Commun. 119, 138–155.

Alladi, T., Chamola, V., Naren, 2020. HARCI: a two-way authentication protocol for three entity healthcare IoT networks. IEEE J. Sel. Area. Commun. 39 (2), 361–369.

Almobaideen, W., Krayshan, R., Allan, M., Saadeh, M., 2017. Internet of Things: geographical Routing based on healthcare centers vicinity for mobile smart tourism destination. Technol. Forecast. Soc. Change 123, 342–350.

Alzahrani, B.A., 2020. Secure and efficient cloud-based IoT authenticated key agreement scheme for e-health wireless sensor networks. Arabian J. Sci. Eng. 46 (4), 3017–3032.

Amin, M., Shehwar, D., Ullah, A., Guarda, T., Tanveer, T.A., Anwar, S., 2020. A deep learning system for health care IoT and smartphone malware detection. Neural Comput. Appl. 32 (21), 1–12.
Arfaoui, A., Kribeche, A., Senouci, S.-M., 2019. Context-aware anonymous authentication protocols in the internet of things dedicated to e-health applications. Comput. Network. 159, 23–36.
Asghari, P., Rahmani, A.M., Javadi, H.H.S., 2018. Service composition approaches in IoT: a systematic review. J. Netw. Comput. Appl. 120, 61–77.
Asghari, P., Rahmani, A.M., Javadi, H.H.S., 2019a. Internet of Things applications: a systematic review. Comput. Network. 148, 241–261.
Asghari, P., Rahmani, A.M., Haj Seyyed Javadi, H., 2019b. A medical monitoring scheme and health-medical service composition model in cloud-based IoT platform. Transactions on Emerging Telecommunications Technologies 30 (6), 3637–3652.
Ashton, K., 2009. That 'internet of things' thing. RFID journal 22 (7), 97–114.
Asif-Ur-Rahman, M., et al., 2019. Towards a heterogeneous mist, fog, and cloud based framework for the internet of healthcare things. IEEE Internet of Things Journal 6 (3), 4049–4062.
Atzori, L., Iera, A., Morabito, G., 2010. The internet of things: a survey. Comput. Network. 54 (15), 2787–2805.
Awaisi, K.S., Hussain, S., Ahmed, M., Khan, A.A., Ahmed, G., 2020. Leveraging IoT and fog computing in healthcare systems, 3. IEEE Internet of Things Magazine, pp. 52–56, 2.
Awan, K.M., et al., 2019. A priority-based congestion-avoidance routing protocol using IoT-based heterogeneous medical sensors for energy efficiency in healthcare wireless body area networks. Int. J. Distributed Sens. Netw. 15 (6), 1–16.
Azimi, I., Pahikkala, T., Rahmani, A.M., Niela-Vilén, H., Axelin, A., Liljeberg, P., 2019. Missing data resilient decision-making for healthcare IoT through personalization: a case study on maternal health. Future Generat. Comput. Syst. 96, 297–308.
Azimi, I., et al., 2017. Hich: hierarchical fog-assisted computing architecture for healthcare iot. ACM Trans. Embed. Comput. Syst. 16 (5), 174–193.
Baek, S., Seo, S.-H., Kim, S., 2016. Preserving patient's anonymity for mobile healthcare system in IoT environment. Int. J. Distributed Sens. Netw. 12 (7), 1–10.
Baker, S.B., Xiang, W., Atkinson, I., 2017. Internet of things for smart healthcare: technologies, challenges, and opportunities. IEEE Access 5, 26521–26544.
Bandopadhaya, S., Dey, R., Suhag, A., 2020. Integrated healthcare monitoring solutions for soldier using the internet of things with distributed computing. Sustainable Computing: Informatics and Systems 26, 100378–100394.
Bazzaz Abkenar, S., Haghi Kashani, M., Mahdipour, E., Jameii, S.M., 2020a. Big data analytics meets social media: a systematic review of techniques, open issues, and future directions. Telematics Inf. 57, 101517–110555.
Bazzaz Abkenar, S., Haghi Kashani, M., Akbari, M., Mahdipour, E., 2020b. Twitter Spam Detection: A Systematic Review. arXiv preprint arXiv:2011.14754, pp. 1–18.
Bazzaz Abkenar, S., Mahdipour, E., Jameii, S.M., Haghi Kashani, M., 2021. A hybrid classification method for Twitter spam detection based on differential evolution and random forest. In: Concurrency and Computation: Practice and Experience. John Wiley & Sons, Inc.
Benadda, B., Beldjilali, B., Mankouri, A., Taleb, O., 2018. Secure IoT solution for wearable health care applications, case study Electric Imp development platform. Int. J. Commun. Syst. 31 (5), 3499–3516.
Bharathi, R., et al., 2020. Energy efficient clustering with disease diagnosis model for IoT based sustainable healthcare systems. Sustainable Computing: Informatics and Systems 28, 1–28.
Bhatia, M., Sood, S.K., 2017. A comprehensive health assessment framework to facilitate IoT-assisted smart workouts: a predictive healthcare perspective. Comput. Ind. 92, 50–66.
Bhatia, M., Kaur, S., Sood, S.K., Behal, V., 2020. Internet of things-inspired healthcare system for urine-based diabetes prediction. Artif. Intell. Med. 107, 101913–101930.
Boussada, R., Hamdane, B., Elhdhili, M.E., Saidane, L.A., 2019. Privacy-preserving aware data transmission for IoT-based e-health. Comput. Network. 162, 106866–106890.
Brereton, P., Kitchenham, B.A., Budgen, D., Turner, M., Khalil, M., 2007. Lessons from applying the systematic literature review process within the software engineering domain. J. Syst. Software 80 (4), 571–583.
Catarinucci, L., et al., 2015. An IoT-aware architecture for smart healthcare systems. IEEE Internet of Things Journal 2 (6), 515–526.
Catherwood, P.A., Steele, D., Little, M., Mccomb, S., Mclaughlin, J., 2018. A community-based IoT personalized wireless healthcare solution trial. IEEE Journal of Translational Engineering in Health and Medicine 6, 1–13.
Chanak, P., Banerjee, I., 2020. Congestion free routing mechanism for IoT-enabled wireless sensor networks for smart healthcare applications. IEEE Trans. Consum. Electron. 66 (3), 223–232.
Chehri, A., Mouftah, H.T., 2020. Internet of Things-integrated IR-UWB technology for healthcare applications. Concurrency Comput. Pract. Ex. 32 (2), e5454.
Chen, S., Xu, H., Liu, D., Hu, B., Wang, H., 2014. A vision of IoT: applications, challenges, and opportunities with China perspective. IEEE Internet of Things Journal 1 (4), 349–359.
Chen, X., Ma, M., Liu, A., 2018. Dynamic power management and adaptive packet size selection for IoT in e-Healthcare. Comput. Electr. Eng. 65, 357–375.
Cutillo, L.A., Manulis, M., Strufe, T., 2010. Security and privacy in online social networks. In: Furht, B. (Ed.), Handbook of Social Network Technologies and Applications. Springer US, Boston, MA, pp. 497–522.
Darwish, A., Hassanien, A.E., Elhoseny, M., Sangaiah, A.K., Muhammad, K., 2017. The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems. Journal of Ambient Intelligence and Humanized Computing 10 (10), 4151–4166.
Deebak, B., Al-Turjman, F., Aloqaily, M., Alfandi, O., 2019. An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT. IEEE Access 7, 135632–135649.
Dey, N., Hassanien, A.E., Bhatt, C., Ashour, A.S., Satapathy, S.C., 2018. Internet of Things and Big Data Analytics toward Next-Generation Intelligence. Springer.
Dhanvijay, M.M., Patil, S.C., 2019. Internet of Things: a survey of enabling technologies in healthcare and its applications. Comput. Network. 153, 113–131.
Dogac, A., Namli, T., Okcan, A., Laleci, G., Kabak, Y., Eichelberg, M., 2007. Key issues of technical interoperability solutions in ehealth and the ride project. In: Software R&D Center, vol. 6531. Dept. of Computer Eng., Middle East Technical University, Ankara, pp. 1–11.
El-Latif, A.A.A., Abd-El-Atty, B., Abou-Nassar, E.M., Venegas-Andraca, S.E., 2020. Controlled alternate quantum walks based privacy preserving healthcare images in internet of things. Opt Laser. Technol. 124, 105942–105965.
Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O.M., Shawkat, S.A., Arunkumar, N., Farouk, A., 2018. Secure medical data transmission model for IoT-based healthcare systems. IEEE Access 6, 20596–20608.
Elmisery, A.M., Rho, S., Botvich, D., 2016. A fog based middleware for automated compliance with OECD privacy principles in internet of healthcare things. IEEE Access 4, 8418–8441.
Elmisery, A.M., Rho, S., Aborizka, M., 2017. A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services. Cluster Comput. 22 (1), 1611–1638.
Elsts, A., et al., 2018. Enabling healthcare in smart homes: the SPHERE IoT network infrastructure. IEEE Commun. Mag. 56 (12), 164–170.
Esmaeili, S., Kamel Tabbakh, S.R., Shakeri, H., 2020. A priority-aware lightweight secure sensing model for body area networks with clinical healthcare applications in Internet of Things. Pervasive Mob. Comput. 69, 1–45.
Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., Mankodiya, K., 2018. Towards fog-driven IoT eHealth: promises and challenges of IoT in medicine and healthcare. Future Generat. Comput. Syst. 78, 659–676.
Fathi, M., Haghi Kashani, M., Jameii, S.M., Mahdipour, E., 2021. Big data analytics in weather forecasting: a systematic review. Archives of Computational Methods in Engineering. Springer.
Fosso Wamba, S., Anand, A., Carter, L., 2013. A literature review of RFID-enabled healthcare applications and issues. Int. J. Inf. Manag. 33 (5), 875–891.
Fotouhi, M., Bayat, M., Das, A.K., Far, H.A.N., Pournaghi, S.M., Doostari, M.A., 2020. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. Comput. Network. 177, 107333–107350.
Fouad, H., Hassanein, A.S., Soliman, A.M., Al-Feel, H., 2020. Analyzing patient health information based on IoT sensor with AI for improving patient assistance in the future direction. Measurement 159, 107757–107772.
Garg, L., Chukwu, E., Nasser, N., Chakraborty, C., Garg, G., 2020. Anonymity preserving IoT-based COVID-19 and other infectious disease contact tracing model. IEEE Access 8, 159402–159414.
Gatouillat, A., Badr, Y., Massot, B., Sejdić, E., 2018. Internet of medical things: a review of recent contributions dealing with cyber-physical systems in medicine. IEEE Internet of Things Journal 5 (5), 3810–3822.
Ghasemi, F., Rezaee, A., Rahmani, A.M., 2019. Structural and behavioral reference model for IoT-based elderly health-care systems in smart home. Int. J. Commun. Syst. 32 (12), 1–21.
Gope, P., Hwang, T., 2016. BSN-Care: a secure IoT-based modern healthcare system using body sensor network. IEEE Sensor. J. 16 (5), 1368–1376.
Gope, P., Gheraibia, Y., Kabir, S., Sikdar, B., 2020. A secure IoT-based modern healthcare system with fault-tolerant decision making process. IEEE Journal of Biomedical and Health Informatics 25 (3), 862–873.
Guo, X., Lin, H., Wu, Y., Peng, M., 2020. A new data clustering strategy for enhancing mutual privacy in healthcare IoT systems. Future Generat. Comput. Syst. 113, 407–417.
Gupta, D.S., Islam, S.H., Obaidat, M.S., Karati, A., Sadoun, B., 2020. LAAC: lightweight lattice-based authentication and access control protocol for E-health systems in IoT environments. IEEE Systems Journal 14 (3), 1–8.
Habibzadeh, H., Dinesh, K., Shishvan, O.R., Boggio-Dandry, A., Sharma, G., Soyata, T., 2020. A survey of healthcare internet of things (HIoT): a clinical perspective. IEEE Internet of Things Journal 7 (1), 53–71.
Haghi Kashani, M., Rahmani, A.M., Jafari Navimipour, N., 2020a. Quality of service-aware approaches in fog computing. Int. J. Commun. Syst. 33 (8), e4340.
Haghi Kashani, M., Ahmadzadeh, A., Mahdipour, E., 2020b. Load Balancing Mechanisms in Fog Computing: A Systematic Review. arXiv preprint arXiv:2011.14706, pp. 1–19.
Hallfors, N.G., et al., 2018. Graphene oxide: nylon ECG sensors for wearable IoT healthcare—nanomaterial and SoC interface. Analog Integr. Circuits Signal Process. 96 (2), 253–260.
Hamza, R., Yan, Z., Muhammad, K., Bellavista, P., Titouna, F., 2020. A privacy-preserving cryptosystem for IoT E-healthcare. Inf. Sci. 527, 493–510.
Hamzei, M., Navimipour, N.J., 2018. Toward efficient service composition techniques in the internet of things. IEEE Internet of Things Journal 5 (5), 3774–3787.
Hao, P., Wang, X., 2017. A PHY-aided secure IoT healthcare system with collaboration of social networks. In: 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall). IEEE, pp. 1–6.
He, D., Zeadally, S., 2015. An analysis of rfid authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. IEEE internet of things journal 2 (1), 72–83.
He, S., Cheng, B., Wang, H., Huang, Y., Chen, J., 2017. Proactive personalized services through fog-cloud computing in large-scale IoT-based healthcare application. China Communications 14 (11), 1–16.

Hogan, W.R., Wagner, M.M., 1997. Accuracy of data in computer-based patient records. J. Am. Med. Inf. Assoc. 4 (5), 342–355.
Hosseinzadeh, M., et al., 2020a. A diagnostic prediction model for chronic kidney disease in internet of things platform. Multimedia Tools and Applications, pp. 1–18.
Hosseinzadeh, M., et al., 2020b. An elderly health monitoring system based on biological and behavioral indicators in internet of things. Journal of Ambient Intelligence and Humanized Computing 11 (10), 1–11.
Hou, J.-L., Yeh, K.-H., 2015. Novel authentication schemes for IoT based healthcare systems. Int. J. Distributed Sens. Netw. 11 (11), 183659.
Hu, L., Qiu, M., Song, J., Hossain, M.S., Ghoneim, A., 2015. Software defined healthcare networks. IEEE Wireless Communications 22 (6), 67–75.
Huang, P., Guo, L., Li, M., Fang, Y., 2019. Practical privacy-preserving ECG-based authentication for IoT-based healthcare. IEEE Internet of Things Journal 6 (5), 9200–9210.
Huifeng, W., Kadry, S.N., Raj, E.D., 2020. Continuous health monitoring of sportsperson using IoT devices based wearable technology. Comput. Commun. 160, 588–595.
Islam, A., Young Shin, S., 2020. A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things. Comput. Electr. Eng. 84, 106627–106642.
Jabbar, S., Ullah, F., Khalid, S., Khan, M., Han, K., 2017. Semantic interoperability in heterogeneous IoT infrastructure for healthcare. Wireless Commun. Mobile Comput. 1–10, 2017, Art no. 9731806.
Jamshidi, P., Ahmad, A., Pahl, C., 2013. Cloud migration research: a systematic review. IEEE Transactions on Cloud Computing 1 (2), 142–157.
Jebadurai, J., Dinesh Peter, J., 2018. Super-resolution of retinal images using multi-kernel SVR for IoT healthcare applications. Future Generat. Comput. Syst. 83, 338–346.
Jeong, Y.-S., Shin, S.-S., 2018. An IoT healthcare service model of a vehicle using implantable devices. Cluster Comput. 21 (1), 1059–1068.
Jia, X., He, D., Kumar, N., Choo, K.-K.R., 2018. Authenticated key agreement scheme for fog-driven IoT healthcare system. Wireless Network 25 (8), 4737–4750.
Jiang, L., Chen, L., Giannetsos, T., Luo, B., Liang, K., Han, J., 2019. Toward practical privacy-preserving processing over encrypted data in IoT: an assistive healthcare use case. IEEE Internet of Things Journal 6 (6), 10177–10190.
Jiang, B., Huang, G., Wang, T., Gui, J., Zhu, X., 2020. Trust based energy efficient data collection with unmanned aerial vehicle in edge network. https://doi.org/10.1002/ett.3942 vol. n/a, no. n/a, p. e3942, 2020/03/17 Transactions on Emerging Telecommunications Technologies.
Kadhim, K.T., Alsahlany, A.M., Wadi, S.M., Kadhum, H.T., 2020. An overview of patient's health status monitoring system based on internet of things (IoT). Wireless Pers. Commun. 114 (3), 2235–2262.
Karimi, Y., Haghi Kashani, M., Akbari, M., Mahdipour, E., 2021. Leveraging big data in smart cities: a systematic review. Concurrency and Computation: Practice and Experience. submitted for publication.
Karimian, N., Tehranipoor, M., Woodard, D., Forte, D., 2019. Unlock your heart: next generation biometric in resource-constrained healthcare systems and IoT. IEEE Access 7, 49135–49149.
Karthigaiveni, M., Indrani, B., 2019. An efficient two-factor authentication scheme with key agreement for IoT based E-health care application using smart card. Journal of Ambient Intelligence and Humanized Computing 10 (10), 1–12.
Kaur, P., Sharma, M., 2020. A smart and promising neurological disorder diagnostic system. Intelligent Data Analysis, pp. 241–264.
Kaur, P., Kumar, R., Kumar, M., 2019. A healthcare monitoring system using random forest and internet of things (IoT). Multimed. Tool. Appl. 78 (14), 19905–19916.
Kavitha, D., Ravikumar, S., 2020. IOT and context-aware learning-based optimal neural network model for real-time health monitoring. Transactions on Emerging Telecommunications Technologies 32 (1), 4132–4150. https://doi.org/10.1002/ett.4132.
Kavitha, K., Sharma, S., 2019. Performance analysis of ACO-based improved virtual machine allocation in cloud for IoT-enabled healthcare. Concurrency Comput. Pract. Ex. 32 (21), 1–12.
Kaw, J.A., Loan, N.A., Parah, S.A., Muhammad, K., Sheikh, J.A., Bhat, G.M., 2019. A reversible and secure patient information hiding system for IoT driven e-health. Int. J. Inf. Manag. 45, 262–275.
Kesavan, R., Arumugam, S., 2020. Adaptive deep convolutional neural network-based secure integration of fog to cloud supported Internet of Things for health monitoring system. Transactions on Emerging Telecommunications Technologies 31 (10), 4104–4120. https://doi.org/10.1002/ett.4104.
Khowaja, S.A., Prabono, A.G., Setiawan, F., Yahya, B.N., Lee, S.-L., 2018. Contextual activity based Healthcare Internet of Things, Services, and People (HIoTSP): an architectural framework for healthcare monitoring using wearable sensors. Comput. Network. 145, 190–206.
Kitchenham, B., Keele, U.K., 2004. Procedures for Performing Systematic Reviews, vol. 33. Keele University, pp. 1–26, 2004.
Kumar, P.M., Gandhi, U.D., 2017. Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application. J. Supercomput. 76 (6), 3963–3983.
Kumar, P., Silambarasan, K., 2019. Enhancing the performance of healthcare service in IoT and cloud using optimized techniques. IETE J. Res. 1–10.
Kumar, P.M., Lokesh, S., Varatharajan, R., Chandra Babu, G., Parthasarathy, P., 2018. Cloud and IoT based disease prediction and diagnosis system for healthcare using Fuzzy neural classifier. Future Generat. Comput. Syst. 86, 527–534.
Laplante, P.A., Kassab, M., Laplante, N.L., Voas, J.M., 2018. Building caring healthcare systems in the internet of things. IEEE Systems Journal 12 (3), 3030–3037.
Li, H., Jing, T., 2019. A lightweight fine-grained searchable encryption scheme in fog-based healthcare IoT networks. Wireless Commun. Mobile Comput. 1–15, 2019.
Li, H., Guo, F., Zhang, W., Wang, J., Xing, J., 2018. "(a,k)-anonymous scheme for privacy-preserving data collection in IoT-based healthcare services systems. J. Med. Syst. 42 (3), 56–65.
Lin, T.-S., Liu, P.-Y., Lin, C.-C., 2019. Home healthcare matching service system using the Internet of Things. Mobile Network. Appl. 24 (3), 736–747.
Lloret, J., Parra, L., Taha, M., Tomás, J., 2017. An architecture and protocol for smart continuous eHealth monitoring using 5G. Comput. Network. 129, 340–351.
Lu, D., Liu, T., 2011. The application of IOT in medical system. In: 2011 IEEE International Symposium on IT in Medicine and Education, vol. 1. IEEE, pp. 272–275.
Mainetti, L., Patrono, L., Vilei, A., 2011. Evolution of wireless sensor networks towards the Internet of Things: a survey. In: SoftCOM 2011, 19th International Conference on Software, Telecommunications and Computer Networks, pp. 1–6.
Manikandan, R., Patan, R., Gandomi, A.H., Sivanesan, P., Kalyanaraman, H., 2020. Hash polynomial two factor decision tree using IoT for smart health care scheduling. Expert Syst. Appl. 141, 112924–112930.
Manishankar, S., Srinithi, C.R., Joseph, D., 2017. Comprehensive study of wireless networks qos parameters and comparing their performance based on real time scenario. In: 2017 International Conference on Innovations in Information, Embedded and Communication Systems. ICIIECS), pp. 1–6.
Manogaran, G., Varatharajan, R., Lopez, D., Kumar, P.M., Sundarasekar, R., Thota, C., 2018. A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system. Future Generat. Comput. Syst. 82, 375–387.
Marengoni, A., et al., 2011. Aging with multimorbidity: a systematic review of the literature. Ageing Res. Rev. 10 (4), 430–439.
Merabet, F., Cherif, A., Belkadi, M., Blazy, O., Conchon, E., Sauveron, D., 2019. New efficient M2C and M2M mutual authentication protocols for IoT-based healthcare applications. Peer-to-Peer Networking and Applications 13 (2), 439–474.
Min, M., et al., 2019. Learning-based privacy-aware offloading for healthcare IoT with energy harvesting. IEEE Internet of Things Journal 6 (3), 4307–4316.
Ming, Y., Yu, X., Shen, X., 2020. Efficient anonymous certificate-based multi- message and multi-receiver signcryption scheme for healthcare internet of things. IEEE Access 8, 153561–153576.
Mohammed, M., Syamsudin, H., Al-Zubaidi, S., Aks, R.R., Yusuf, E., 2020. Novel COVID-19 detection and diagnosis system using IOT based smart helmet. Int. J. Psychosoc. Rehabil. 24 (7), 2296–2303.
Muthu, B., et al., 2020. IOT based wearable sensor for diseases prediction and symptom analysis in healthcare sector. Peer-to-Peer Networking and Applications 13 (6), 2123–2134.
Najafizadeh, A., Kashani, M.H., 2011. A novel intelligent mechanism for energy efficiency in hierarchical WSNs. International Journal of Advanced Engineering Sciences and Technologies 10 (1), 139–144.
Najafizadeh, A., Salajegheh, A., Rahmani, A.M., Sahafi, A., 2021. Privacy-preserving for the Internet of Things in multi-objective task scheduling in cloud-fog computing using goal programming approach. Peer-to-Peer Networking and Applications. submitted for publication.
Nasajpour, M., Pouriyeh, S., Parizi, R.M., Dorodchi, M., Valero, M., Arabnia, H.R., 2020. Internet of things for current COVID-19 and future pandemics: an exploratory study. Journal of Healthcare Informatics Research 4 (4), 325–364.
Niitsu, K., et al., 2018. A self-powered supply-sensing biosensor platform using bio fuel cell and low-voltage, low-cost CMOS supply-controlled ring oscillator with inductive-coupling transmitter for healthcare IoT. IEEE Transactions on Circuits and Systems I: Regular Papers 65 (9), 2784–2796.
Nikravan, M., Jameii, S.M., Kashani, M.H., 2011. An intelligent energy efficient QoS-routing scheme for WSN. International Journal of advanced Engineering sciences and Technologies 8 (1), 121–124.
Onasanya, A., Elshakankiri, M., 2019. Smart integrated IoT healthcare system for cancer care. Wireless Network 25 (1), 1–16.
Onasanya, A., Lakkis, S., Elshakankiri, M., 2019. Implementing IoT/WSN based smart saskatchewan healthcare system. Wireless Network 25 (7), 3999–4020.
Pal, S., Hitchens, M., Varadharajan, V., Rabehaja, T., 2019. Policy-based access control for constrained healthcare resources in the context of the Internet of Things. J. Netw. Comput. Appl. 139, 57–74.
Patan, R., Pradeep Ghantasala, G.S., Sekaran, R., Gupta, D., Ramachandran, M., 2020. Smart healthcare and quality of service in IoT using grey filter convolutional based cyber physical system. Sustainable Cities and Society 59, 102141–102161.
Pramanik, P.K.D., Solanki, A., Debnath, A., Nayyar, A., El-Sappagh, S., Kwak, K., 2020. Advancing modern healthcare with nanotechnology, nanobiosensors, and internet of nano things: taxonomies, applications, architecture, and challenges. IEEE Access 8, 65230–65266.
Qadri, Y.A., Nauman, A., Zikria, Y.B., Vasilakos, A.V., Kim, S.W., 2020. The future of healthcare internet of things: a survey of emerging technologies. IEEE Communications Surveys & Tutorials 22 (2), 1121–1167.
Qi, J., Yang, P., Min, G., Amft, O., Dong, F., Xu, L., 2017. Advanced internet of things for personalised healthcare systems: a survey. Pervasive Mob. Comput. 41, 132–149.
Qi, J., Yang, P., Waraich, A., Deng, Z., Zhao, Y., Yang, Y., 2018. Examining sensor-based physical activity recognition and monitoring for healthcare using Internet of Things: a systematic review. J. Biomed. Inf. 87, 138–153.
Qiu, T., Liu, X., Han, M., Li, M., Zhang, Y., 2017. SRTS: a self-recoverable time synchronization for sensor networks of healthcare IoT. Comput. Network. 129, 481–492.
Rahimi, M., Songhorabadi, M., Kashani, M.H., 2020. Fog-based smart homes: a systematic review. J. Netw. Comput. Appl. 153, 102531.

Rahmani, A.M., Babaei, Z., Souri, A., 2020. Event-driven IoT architecture for data analysis of reliable healthcare application using complex event processing. Cluster Comput. 23 (4), 1–14.
Rahmani, A.M., et al., 2018. Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: a fog computing approach. Future Generat. Comput. Syst. 78, 641–658.
Rajan, J.P., Rajan, S.E., Martis, R.J., Panigrahi, B., 2020. Fog computing employed computer aided cancer classification system using deep neural network in internet of things based healthcare system. J. Med. Syst. 44 (2), 34–43.
Rajan Jeyaraj, P., Nadar, E.R.S., 2019. Smart-monitor: patient monitoring system for IoT-based healthcare system using deep learning. IETE J. Res. 1–8.
Rajan Jeyaraj, P., Nadar, E.R.S., 2020. Atrial fibrillation classification using deep learning algorithm in Internet of Things–based smart healthcare system. Health Inf. J. 26 (3), 1827–1840.
Ramírez López, L.J., Rodriguez Garcia, A., Puerta Aponte, G., 2019. Internet of things in healthcare monitoring to enhance acquisition performance of respiratory disorder sensors. Int. J. Distributed Sens. Netw. 15 (5), 1–10.
Rani, S.S., Alzubi, J.A., Lakshmanaprabu, S., Gupta, D., Manikandan, R., 2019. Optimal users based secure data transmission on the internet of healthcare things (IoHT) with lightweight block ciphers. Multimed. Tool. Appl. 78 (9), 35405–35424.
Rathee, G., Sharma, A., Saini, H., Kumar, R., Iqbal, R., 2019. A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. Multimed. Tool. Appl. 79 (11), 9711–9733.
Ray, P.P., Dash, D., De, D., 2018. Approximation of fruit ripening quality index for IoT based assistive e-healthcare. Microsyst. Technol. 25 (8), 3027–3036.
Ray, P.P., Dash, D., De, D., 2019a. Internet of things-based real-time model study on e-healthcare: device, message service and dew computing. Comput. Network. 149, 226–239.
Ray, P.P., Dash, D., De, D., 2019b. Edge computing for Internet of Things: a survey, e-healthcare case study and future direction. J. Netw. Comput. Appl. 140, 1–22.
Ray, P.P., Dash, D., De, D., 2019c. Analysis and monitoring of IoT-assisted human physiological galvanic skin responsefactor for smart e-healthcare. Sens. Rev. 39 (4), 525–541.
Ray, P.P., Thapa, N., Dash, D., De, D., 2019d. Novel implementation of IoT based non-invasive sensor system for real-time monitoring of intravenous fluid level for assistive e-healthcare. Circ. World 45 (3), 109–123.
Ray, P.P., Dash, D., De, D., 2019e. Real-time event-driven sensor data analytics at the edge-Internet of Things for smart personal healthcare. J. Supercomput. 76 (9), 6648–6668.
Renner, S., 2001. A community of interest approach to data interoperability. In: Federal Database Colloquium, vol. 1. CiteSeerX, San Diego, CA, pp. 1–7.
Ruan, L., Dias, M.P.I., Wong, E., 2017. Towards tactile internet capable E-health: a delay performance study of downlink-dominated SmartBANs. GLOBECOM 2017 - 2017 IEEE Global Communications Conference, pp. 1–6.
Saha, R., Kumar, G., Rai, M.K., Thomas, R., Lim, S., 2019. Privacy ensured –Healthcare for fog-enhanced IoT based applications. IEEE Access 7, 44536–44543.
Saheb, T., Izadi, L., 2019. Paradigm of IoT big data analytics in healthcare industry: a review of scientific literature and mapping of research trends. Telematics Inf. 41 (1), 70–85.
Sahoo, S.S., Mohanty, S., Majhi, B., 2020. A secure three factor based authentication scheme for health care systems using IoT enabled devices. Journal of Ambient Intelligence and Humanized Computing 12 (1), 1419–1434.
Sakiz, F., Sen, S., 2017. A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. Ad Hoc Netw. 61, 33–50.
Santos, M.A.G., Munoz, R., Olivares, R., Filho, P.P.R., Ser, J.D., Albuquerque, V.H. C.d., 2020. Online heart monitoring systems on the internet of health things environments: a survey, a reference model and an outlook. Inf. Fusion 53, 222–239.
Satpathy, S., Mohan, P., Das, S., Debbarma, S., 2019. A new healthcare diagnosis system using an IoT-based fuzzy classifier with FPGA. J. Supercomput. 76 (9), 5849–5861.
Sengupta, S., Bhunia, S.S., 2020. Secure data management in cloudlet assisted IoT enabled e-health framework in smart city. IEEE Sensor. J. 20 (16), 9581–9588.
Sharavana Kumar, M.G., Sarma Dhulipala, V.R., 2020. Fuzzy allocation model for health care data management on IoT assisted wearable sensor platform. Measurement 166, 1–24.
Sharma, G., Kalra, S., 2019. A lightweight user authentication scheme for cloud-IoT based healthcare services. Iranian Journal of Science and Technology, Transactions of Electrical Engineering 43 (1), 619–636.
Sharma, S., Dudeja, R.K., Aujla, G.S., Bali, R.S., Kumar, N., 2020. DeTrAs: deep learning-based healthcare framework for IoT-based assistance of Alzheimer patients. Neural Comput. Appl. 32 (17), 1–13.
Sheikh Sofla, M., Haghi Kashani, M., Mahdipour, E., Faghih Mirzaee, R., 2021. Towards effective offloading mechanisms in fog computing: a systematic survey. Multimedia Tools and Applications. Springer. Submitted for publication.
Singh, R.P., Javaid, M., Haleem, A., Suman, R., 2020. Internet of things (IoT) applications to fight against COVID-19 pandemic. Diabetes & Metabolic Syndrome: Clin. Res. Rev. 14 (4), 521–524.
Somasundaram, R., Thirugnanam, M., 2020. Review of security challenges in healthcare internet of things. Wireless Network 26 (1), 1–7.
Songhorabadi, M., Rahimi, M., Farid, A.M.M., Kashani, M.H., 2020. Fog Computing Approaches in Smart Cities: A State-Of-The-Art Review. arXiv preprint arXiv: 2011.14732, pp. 1–19.
Sood, S.K., Mahajan, I., 2019. IoT-fog based healthcare framework to identify and control hypertension attack. IEEE Internet of Things Journal 6 (2), 1920–1927.
Subramaniyaswamy, V., et al., 2018. An ontology-driven personalized food recommendation in IoT-based healthcare system. J. Supercomput. 75 (6), 3184–3216.
Sultan, N., 2014. Making use of cloud computing for healthcare provision: opportunities and challenges. Int. J. Inf. Manag. 34 (2), 177–184.
Sun, J., Xiong, H., Liu, X., Zhang, Y., Nie, X., Deng, R.H., 2020. Lightweight and privacy-aware fine-grained access control for IoT-oriented smart health. IEEE Internet of Things Journal 7 (7), 6566–6575.
Suresh, A., Udendhran, R., Balamurgan, M., Varatharajan, R., 2019. A novel internet of things framework integrated with real time monitoring for intelligent healthcare environment. J. Med. Syst. 43 (6), 165–175.
Tan, E., Halim, Z.A., 2019. Health care monitoring system and analytics based on internet of things framework. IETE J. Res. 65 (5), 653–660.
Tang, W., Ren, J., Deng, K., Zhang, Y., 2019. Secure data aggregation of lightweight E-healthcare IoT devices with fair incentives. IEEE Internet of Things Journal 6 (5), 8714–8726.
Tao, H., Bhuiyan, M.Z.A., Abdalla, A.N., Hassan, M.M., Zain, J.M., Hayajneh, T., 2019. Secured data collection with hardware-based ciphers for IoT-based healthcare. IEEE Internet of Things Journal 6 (1), 410–420.
Tekeste, T., Saleh, H., Mohammad, B., Ismail, M., 2019. Ultra-low power QRS detection and ECG compression architecture for IoT healthcare devices. IEEE Transactions on Circuits and Systems I: Regular Papers 66 (2), 669–679.
Tsiounia, K., Dimitrioglou, N.G., Kardaras, D., Barbounaki, S.G., 2019. A process modelling and analytic hierarchy process approach to investigate the potential of the IoT in health services. In: World Congress on Medical Physics and Biomedical Engineering 2018. Springer Singapore, Singapore, pp. 381–386.
Tuli, S., et al., 2020. HealthFog: an ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated IoT and fog computing environments. Future Generat. Comput. Syst. 104, 187–200.
Ullah, F., Habib, M.A., Farhan, M., Khalid, S., Durrani, M.Y., Jabbar, S., 2017. Semantic interoperability for big-data in heterogeneous IoT infrastructure for healthcare. Sustainable cities and society 34, 90–96.
Ullah, I., Amin, N.U., Khan, M.A., Khattak, H., Kumari, S., 2020a. An efficient and provable secure certificate-based combined signature, encryption and signcryption scheme for internet of things (IoT) in mobile health (M-Health) system. J. Med. Syst. 45 (1), 1–14.
Ullah, A., Said, G., Sher, M., Ning, H., 2020b. Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN. Peer-to-Peer Networking and Applications 13 (1), 163–174.
Usak, M., Kubiatko, M., Shabbir, M.S., Viktorovna Dudnik, O., Jermsittiparsert, K., Rajabion, L., 2020. Health care service delivery based on the Internet of things: a systematic and comprehensive study. Int. J. Commun. Syst. 33 (2), 4179–4196. https://doi.org/10.1002/dac.4179.
Vaishnavi, S., Sethukarasi, T., 2020. SybilWatch: a novel approach to detect Sybil attack in IoT based smart health care. Journal of Ambient Intelligence and Humanized Computing 11 (6), 1–15.
Vedaei, S.S., et al., 2020. COVID-SAFE: an IoT-based system for automated health monitoring and surveillance in post-pandemic life. IEEE Access 8, 188538–188551.
Vedaraj, M., Ezhumalai, P., 2020. HERDE-MSNB: a predictive security architecture for IoT health cloud system. Journal of Ambient Intelligence and Humanized Computing 11 (8), 1–10.
Verma, P., Sood, S.K., 2018. Cloud-centric IoT based disease diagnosis healthcare framework. J. Parallel Distr. Comput. 116, 27–38.
Verma, P., Sood, S.K., Kalra, S., 2018. Cloud-centric IoT based student healthcare monitoring framework. Journal of Ambient Intelligence and Humanized Computing 9 (5), 1293–1309.
Vilela, P.H., Rodrigues, J.J., Solic, P., Saleem, K., Furtado, V., 2019. Performance evaluation of a Fog-assisted IoT solution for e-Health applications. Future Generat. Comput. Syst. 97, 379–386.
Wang, X., Cai, S., 2020. Secure healthcare monitoring framework integrating NDN-based IoT with edge cloud. Future Generat. Comput. Syst. 112, 320–329.
Wang, X., Li, Y., 2020. Fog-assisted content-centric healthcare IoT. IEEE Internet of Things Magazine 3 (3), 90–93.
Wilson, D., 2017. An overview of the application of wearable technology to nursing practice. Nursing forum, 52. Wiley Online Library, pp. 124–132, 2.
Woo, M.W., Lee, J., Park, K., 2018. A reliable IoT system for personal healthcare devices. Future Generat. Comput. Syst. 78, 626–640.
Wu, M., Lu, T.-J., Ling, F.-Y., Sun, J., Du, H.-Y., 2010. Research on the architecture of internet of things. In: 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), vol. 5. IEEE, pp. 484–487.
Wu, T., Wu, F., Redouté, J., Yuce, M.R., 2017. An autonomous wireless body area network implementation towards IoT connected healthcare applications. IEEE Access 5, 11413–11422.
Wu, T., Redouté, J.-M., Yuce, M.R., 2018. A wireless implantable sensor design with subcutaneous energy harvesting for long-term IoT healthcare applications. IEEE Access 6, 35801–35808.
Wu, T., Wu, F., Qiu, C., Redouté, J.M., Yuce, M.R., 2020. A rigid-flex wearable health monitoring sensor patch for IoT-connected healthcare applications. IEEE Internet of Things Journal 7 (8), 6932–6945.
Xu, G., 2020. IoT-assisted ECG monitoring framework with secure data transmission for health care applications. IEEE Access 8, 74586–74594.
Xu, S., Li, Y., Deng, R., Zhang, Y., Luo, X., Liu, X., 2019. Lightweight and expressive fine-grained access control for healthcare internet-of-things. IEEE Transactions on Cloud Computing 14 (8), 1–17.
Yang, Z., Zhou, Q., Lei, L., Zheng, K., Xiang, W., 2016. An IoT-cloud based wearable ECG monitoring system for smart healthcare. J. Med. Syst. 40 (12), 286–297.
Yang, Y., Liu, X., Deng, R.H., 2018. Lightweight break-glass access control system for healthcare internet-of-things. IEEE Transactions on Industrial Informatics 14 (8), 3610–3617.

Yang, Y., Zheng, X., Guo, W., Liu, X., Chang, V., 2019. Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. Inf. Sci. 479, 567–592.
Yang, P., et al., 2018. Lifelogging data validation model for internet of things enabled personalized healthcare. IEEE Transactions on Systems, Man, and Cybernetics: Systems 48 (1), 50–64.
Yeh, K.-H., 2016. A secure IoT-based healthcare system with body sensor networks. IEEE Access 4, 10288–10299.
Yi, C., Cai, J., 2019. A truthful mechanism for scheduling delay-constrained wireless transmissions in IoT-based healthcare networks. IEEE Trans. Wireless Commun. 18 (2), 912–925.
Zgheib, R., Kristiansen, S., Conchon, E., Plageman, T., Goebel, V., Bastide, R., 2020. A scalable semantic framework for IoT healthcare applications. Journal of Ambient Intelligence and Humanized Computing 11 (6), 1–19.
Zhou, W., Piramuthu, S., 2018. IoT security perspective of a flexible healthcare supply chain. Inf. Technol. Manag. 19 (3), 141–153.
Zou, N., Liang, S., He, D., 2020. Issues and challenges of user and data interaction in healthcare-related IoT: a systematic review, 38. Library Hi Tech, pp. 769–782, 4.

Mostafa Haghi Kashani received his B.S. in Computer Engineering from Kashan Branch of IAU, Iran, in 1999 and the M.S. in Computer Software Engineering from South Tehran Branch of IAU, Iran in 2002. He is currently a full-time Ph.D. Candidate in Computer Engineering-Software Systems at Science and Research Branch of IAU, Tehran, Iran. He is a researcher and lecturer in the Department of Computer Engineering at the IAU University. His research interests include distributed systems, fog computing, IoT, healthcare, big data, and evolutionary computing. He serves as an Editor for Frontiers in Big Data and Frontiers in Artificial Intelligence. He has acted as a reviewer in several international journals, including the IEEE Transactions on Industrial Informatics, Journal of Supercomputing (Springer), the International Journal of Communication Systems (Wiley), Multimedia Tools and Applications (Springer), and other top journals in the field.

Mona Madanipour received her B.S. degree in Computer Science from Shahed University, Tehran, Iran, in 2014; she is an M.S. student in Information Technology, Computer Networks, in Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran. Her research interests include IoT, e-Health, fog computing, recommender systems, machine learning, and data mining.

Mohammad Nikravan received his B.Sc. in Computer Software Engineering from the Islamic Azad University, Mashhad Branch, Iran, in 2002. He also received M.Sc. degree in Computer Software from the South Tehran Branch, Islamic Azad University, Tehran, Iran in 2005 and Ph.D. degree in Computer Software from the Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran in 2018. Currently, he is an assistant professor of the Department of Computer Engineering Shahr-e-Qods Branch, Islamic Azad University, Iran. His research interests include the Internet of things, 6LoWPAN networks and cryptography, and network security.

Parvaneh Asghari is a full-time faculty member and Assistant Professor in the Department of Computer Engineering at IAU, Central Tehran Branch (IAUCTB). She received her B.S. degree in Computer Software Engineering from Sharif University of Technology, Tehran, Iran, in 1994, her M.Sc. degree in Computer Software Engineering from Iran University of Science & Technology, Tehran, Iran in 1997, and her Ph.D. degree in Computer Software Engineering from IAU, Science and Research Branch, Tehran, Iran, in 2019. Her research interests are in areas of distributed systems, IoT, healthcare, cloud computing, and service-oriented computing. She also serves as a reviewer for various journals such as IEEE Communications Surveys and Tutorials, the Journal of Network and Computer Applications, Cluster Computing, IEEE Access, Human-centric Computing and Information Sciences, IET communications, RVT, and many other top journals in the field.

Ebrahim Mahdipour received the B.S. degree in computer engineering, specialized in hardware engineering, from the Dezful Branch, Islamic Azad University, Dezful, Iran, in 2003, the M.S. degree in computer engineering, specialized in computer architecture, and the Ph.D. degree in computer engineering, specialized in computer architecture, from the Science and Research Branch, Islamic Azad University, Tehran, Iran, in 2006 and 2012. He is the founding director of the Cyber Security Research Center, and he is currently an Assistance Professor with the Department of Computer Engineering, Science and Research Branch, Islamic Azad University. His research interests include cyber security, blockchain, and big data.