Review

Application of internet of things in healthcare domain

Khaled H. Almotairi[1]

Received: 7 September 2022 / Accepted: 4 October 2022
Published online: 6 December 2022

Abstract
Internet of things (IoT) enables machine-to-machine, human-to-human and machine-to-human interaction. Recent advancement in IoT systems has positively impacted the daily activities of humans, from accessing information to the delivery of service in real-time. This has improved healthcare management and services, especially in medical hospitals, for effective and timely access to diagnostic information and treatment of patients. Several existing research mainly focused on the design of IoT architecture, its challenges, and benefits to human society with minor or without considering applying IoT in the healthcare domain. To bridge this gap, this study investigates the implications of IoT integration in the healthcare management domain. It presents a detailed discussion on IoT utilization to improve the functionalities of hospital management system. It also discusses some potential emerging innovations that aids the development and application of IoT in hospital management systems. Investigations show that healthcare personnel can administer treatments to patients anytime–anywhere. Patients, especially the elderly are administered treatment, as well as monitoring their wellbeing while at home with the support of wearable sensor devices. Also, some of the challenges that impedes the integration of IoT application into healthcare domain includes generation of irrelevant huge amount of data, issues of security and privacy of patient information and high cost of IoT adoption. Furthermore, the future research trends in adoption of IoT to improve healthcare domain includes stroke and epileptic seizure predictions and prosthetic sensors which is used to retrieve relevant data or information to aid the treatment of a patient in real-time.

Keywords Healthcare · Security · Smart equipment · Hospital Management · Internet of things (IoT) · Blockchain · Machine learning · Artificial intelligence

1 Introduction

There have been rapid advances in the management of healthcare, based on hospital systems and related medical science disciplines. A few studies have attributed this current development in the healthcare sector, to rapid increase in global population density, aging factors, and technological advancement [1]. Considering a recent aging and health study conducted by the World Health Organization (WHO), the number of people aged 60 years and above (900 million in the year 2015) is estimated to increase to over 2 billion before the year 2050, increasing approximately from 12 to 22% on aggregate based on global population [2]. Therefore, the rapid increase in demographic shift becomes a burden and challenge to healthcare practitioners. This is due to limited healthcare resources available in hospital to meet the influx of patients. However, the increase in the number of healthcare practitioners has paved the way for patients to make decisive decisions based on the selection of medical specialists [3]. Healthcare specialists and providers are consistently under pressure to

✉ Khaled H. Almotairi, khmotairi@uqu.edu.sa | [1]Computer Engineering Department, Computer and Information Systems College, Umm Al-Qura University, Makkah 21955, Saudi Arabia.

J. Umm Al-Qura Univ. Eng.Archit. (2023) 14:1–12 | https://doi.org/10.1007/s43995-022-00008-8

deliver better healthcare services with limited resources at their disposal. Hence, there is an urgent need to manage costs, and provide quality, efficient and reliable healthcare services to the populace [4, 5] This can only be achieved by applying a real-time system for the management and delivery of healthcare related services to patients (such as the elderly) that are immobile and afflicted with chronic diseases that require constant monitoring. In addition, young people require quality healthcare services to improve their life expectancy as they grow older. Therefore, these can be achieved by deploying Internet of things (IoT) enabled Health systems, for the delivery of timely and quality healthcare services to patients across the globe. Even though, IoT has been applied in other fields such as transportation and logistics [6].

The term IoT refers to several physical devices (sensors data, intelligence services, data processing, software, and smart applications, etc.) that are connected to the internet for storing, retrieval, sharing and aggregation of data [7]. Internet can be leveraged as a medium of interaction between prospective patients and medical facilities, at any-time and any-where for the delivery of quality healthcare [8]. Therefore, healthcare practitioner or institution can create a transparent, effective [9]. Also, it can create real-time healthcare delivery model with the implementation of IoT technology [10].

Moreover, IoT-based healthcare systems has improved health service delivery exclusively from a conventional healthcare point of view, providing a modern real-time healthcare system. Consequently, traditional medicine has been modernized with the support of biotechnology that act as key enablers in the emergence of smart healthcare enabled hospital management systems. Hence, the smart healthcare-based hospital management system emerges as the better option for the delivery of healthcare services due to its integration with IoT technologies [11].

The technology that supports the realization of a smart healthcare enabled hospital management system is sometimes described as the Internet of Medical Things (IoMT) [5]. It consists of utilizing internet-enabled smart devices and wearable medical sensors to monitor patient health, check adherence to prescriptions, predict an impending heart attack and retrieve timely diagnostic information [12].

There are various existing literature on overview of Internet of Things technologies and its applications. For instance, Colakovic and Hadzialic [13] investigated the enabling IoT technological challenges and open research issues. It discusses various versions of related IoT technologies to enable better understanding of its features. Consequently, a survey was conducted to provide an insight into IoT emerging technologies and identify the most relevant among them. Detailed open issues and challenges to be resolved by future research studies were presented.

Akhigbe et al. [14] presented a review on the application of IoT technologies to Livestock management. The IoT ecosystems were vividly identified, with an improved architecture and its technicalities. Furthermore, the current state, opportunities and expected research trends of IoT enabled Livestock management system was discussed. Findings show that the proliferation of IoT data from livestock is a major contributor. As conventional methods of reactive data processing will be replaced with proactive (IoT data) methods to provide insight about animal processes [15]. Javed et al. [16] presented a survey on Internet of Things operating systems support, applications and challenges. It provides a comprehensive comparison of operating systems designed for IoT devices based on their architecture, power, scheduling and memory management approaches, and programming models. It also highlights the networking methods together with related features needed for IoT enabled applications. In addition, several case studies and challenges in IoT domains are discussed. Pirmagomedov and Koucheryavy [17] presented a comprehensive survey on IoT technologies for an Augmented Human. It discusses the concepts of an augmented human and highlights notable research issues raised by such systems. In addition, a detailed emerging IoT enabled human augmentation, devices and design approaches, together with connectivity methods and security challenges is discussed [18].

Vo et al. [19] presented a review on Internet of things enabled ocean controlled environmental pollution. It initially identifies the applications of an intelligent environment as the basis for analysing emerging IoT approaches consisting of big data and artificial intelligence for monitoring and controlling pollution in marine environments. Furthermore, the prospective opportunities and challenges vital to this field of research were deliberated, which mainly considered the applications of IoT-big data systems for the protection of the ocean environment. Gomez-Chalbla et al. [20] presented a systematic review on IoT Applications in Agriculture. It highlights various type of IoT-enabled software application in agriculture existing in the market, such as soil sensors, together with the advantages offered by the technologies.

The existing research in this field as extensively discussed above mainly focuses on IoT related technologies, challenges and potential future research trends. They also discuss IoT applications in the agriculture and ocean environment without considering IoT enabled healthcare systems deployed in medical hospitals to improve real-time information that leads to prompt treatment of critical diseases. Therefore, this study addresses the gap of the existing research by investigating the application of IoT

enabled technology in medical hospitals. The contributions of this research are highlighted as follows:

- The purpose of developing IoT-enabled Smart Healthcare as well as its importance were highlighted and discussed.
- A detailed utilization of IoT-enabled technologies in healthcare, especially in medical hospitals is presented in this research.
- The challenges such security and privacy were identified and extensively discussed which pave the way for future research directions in this field.

The main benefit of this research paper is to provide a critical analysis that gives information to academic researchers regarding the current status of IoT technologies in healthcare-enabled hospital management domain, as well as critical issues to be addressed in the future. Hence, the structure of this research paper is as follows. Section 2 presents overview of IoT and healthcare system. The overview put forth more information regarding paradigm shift in smart healthcare with advantages of IoT-enabled healthcare system. In Sect. 3, the detailed discussion on the purpose and importance of implementing IoT-enabled smart healthcare is presented. The section further explained the scope of utilization of IoT in hospital management system. Section 4 presents discussion on future research trends in IoT-enabled healthcare infrastructure. Some of the research trends include prediction of stroke and epileptic seizure, prosthetics sensors, precision in-vivo procedure and Blockchain. In Sect. 5, the current challenges in IoT-enabled healthcare application are presented. The challenges focused on two aspects namely, infrastructure and security challenges. The conclusion of the study is presented in Sect. 6, which contains remarks and recommendation on paradigm shift in IoT-enabled healthcare system.

2 Overview of IoT and healthcare system

The IoT paradigm enables smart devices (mobile phones, sensor device and Raspberry Pi) to sense, monitor and react to the environment. It aims to achieve a wider connection range by connecting numerous devices to the internet at a particular time [21–23]. Therefore, both human-to-machine and machine-to-machine interactions are feasible. This means that humans can interact with a machine for the purpose of performing healthcare related tasks such as surgery on patients, monitoring of prospective patients in their place of residence, and monitoring of hospital legacy facilities and environments in real-time [24–28]. In addition, machines interact with their counterparts for information storing and retrieval, such as sensors transmitting its information to a cloudlet system for temporary storage [29, 30]. A typical example of an IoT-enabled healthcare platform is depicted Fig. 1.

It shows the four basic components that constitutes a conventional IoT-enabled Healthcare infrastructure. The hospital is the first component which accommodates both healthcare practitioners and In/Out patients [31, 32]. IoT applications enables hospital management to closely observe or monitor the well-being and the recovery process of out-patients (already discharged from the hospital ward) in their respective homes in real-time. This can be achieved by wearable or embedded medical body

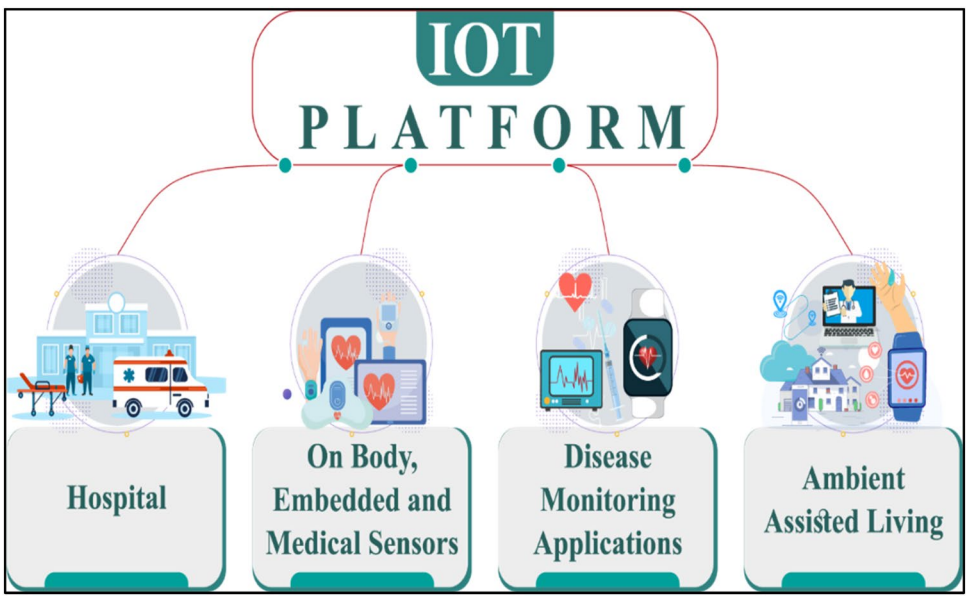

Fig. 1 IoT and its associated healthcare platform

sensors. The retrieved sensor readings are manipulated and transformed into useful information with the support of machine learning techniques together with application software. Thus, to assist the medical staff in the hospital facility visualize the current health status of an out-patient residing at his/her home. For instance, if the health of an out-patient is observed to be deteriorating or in critical condition, such patients are transported to the hospital ward by an emergency vehicle within a limited period of time [33].

Conversely, out-patients who are not under close monitoring or have recovered from their illness may be provided with IoT-enabled ambient assistive living devices. The ambient assistive living device helps the out-patient or individual to manage his/her well-being in real-time. For instance, it monitors and informs the individual of the number of calories burnt-, the sugar content in the body and the heart-rate. Therefore, a patient or individual can manage any unforeseen health issues with the available information retrieved from the ambient assistive IoT devices. Thus, enhancing the patient's well-being, as well as providing care givers with the necessary tools and timely information needed for optimal health services to the general public, which is generally known as smart healthcare.

2.1 Smart healthcare

Smart healthcare originates from the concept of "Smart Planet" introduced in 2009 by IBM [34]. The Smart Planet is described as an intelligent infrastructure that utilizes sensors to retrieve information. The retrieved information is transmitted via IoT related devices to the Cloud Data-Centre where it a processed into useful information and accessed by healthcare providers and authorized patients. In addition, the emergence of smart healthcare was motivated by the concept that patients expect healthcare providers to render quality and timely services to them anytime–anywhere. Many authors classified smart healthcare as patient-centric facilities connected to an ecosystem where healthcare programs are delivered at different locations, including patient's homes and hospital wards. Smart healthcare is capable of facilitating affective communication between patients and management of a healthcare facility [35–40]. It assists healthcare stakeholders in making intelligent choices, enables logical sharing of healthcare facilities, and ensures quality healthcare services. Furthermore, smart healthcare refers to an advanced form of data interpretation for medical purposes [41].

Conversely, an IoT-enabled healthcare management service is a form of heterogeneous computing. This is because of the type of wireless communication system of applications and devices that serve as connection buses between patients and healthcare officials. The services include diagnosing, monitoring, tracking, and storing vital statistical and medical information [42, 43]. Some of the smart healthcare application opportunities includes handsets that measure brainwaves, clothes embedded with sensing devices, blood pressure (BP) monitors, glucose monitoring [34], Electrocardiogram (ECG) monitoring, and pulse oximeters. Other application areas are sensors embedded in medical equipment, dispensing systems, surgical robots, device implants, and any wearable devices. A good example of smart healthcare is the provisioning of a smart bed provided by Ably Medical Centre in Norway. The smart bed is embedded with sensors to measure vital signs, weight, heart beat rate and blood pressure. It has the ability to inform medical health care providers of the current status of a patient's condition (either its deteriorating or responding to treatment). In addition, it prevents patients from falling or turns them to alleviate pressure points on their bodies without human assistance.

2.2 Advantages of IoT-enabled healthcare system

The advantages of IoT-enabled smart healthcare systems includes "better treatment, optimal disease control, maintenance and safety of medical facilities" [44, 45] as depicted in Fig. 2.

Better treatment is achieved with the support of error free diagnostic information captured and processed by IoT devices. When patients experience better or quality treatment, it enhances their confidence and trust in the healthcare personnel and facilities of that hospital. In addition, the general public can have access to medical advice at an affordable rate, anytime–anywhere in real-time via the internet. Smart healthcare also enables the maintenance and safety of healthcare facilities by constant monitoring with the assistance of embedded camera sensor devices. Furthermore, it assists the elderly in managing critical health challenges without frequent visits to the hospital for checkups by doctor/nurses.

3 Scope of utilization of IoT in hospital management system

The Internet of Things technology have gained a developmental stride in the digital world, deployed in various units and departments in the healthcare domain, resulting in better treatment and efficient healthcare service delivery in real time. The health sector is known for its constant exploration of ways to enhance its services, mitigate costs, and improve the integrity of health services rendered. Therefore, there is the possibility of an exponential increase in the rate at which the healthcare system relies

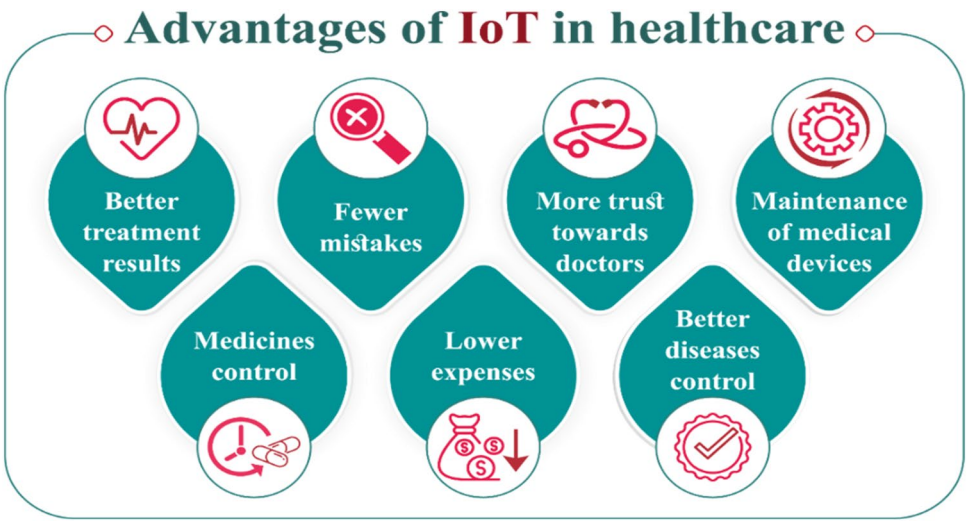

Fig. 2 Advantages of IoT in healthcare

on this technology [46, 47]. This is due to the fact that it becomes easy to obtain tips for healthy living with the support of an IoT-enabled healthcare system. This minimizes cost, improves patients experience and satisfaction. Furthermore, IoT-based systems can be applied for remote monitoring of physiological status in patients that require continuous monitoring [48–50].

Advancements in the smart healthcare system can be achieved through collaboration among different IoT architectures [51]. To examine the health condition of a patient, IoT-driven applications can be useful to generate a comprehensive entity with the convergence of different devices. Hence, the current technology in the hospital management system and overall medical activities are improved with the IoT system. The capability to easily reach out to healthcare professionals and medical consultants is rapidly advancing. Data gathered from large areas of real-world scenarios increase both the size and accuracy of medical data [52]. Moreover, the precision of healthcare delivery is equally enhanced by incorporating a higher number of modern technologies in the hospital management system. Some applications of the IoT technology for smart hospital management systems is presented in Table 1.

Table 1 Applications of IoT for smart healthcare system

References	Architecture	Application/use case/benefits to smart healthcare system
[77]	Based on expert systems used in clinical diagnosis. The IoT architecture fuses perception/sensor, application, and network layers	Improved treatment, assessment, and diagnosis of psoriasis Reduction in expenses that accompany the transfer of patients from one clinic to another owing to improper diagnosis and/or treatment of psoriasis
[78]	Adopted the use of a visual tool for achieving differential diagnosis based on nearest neighbor classifier, voting feature intervals-5 and naive Bayesian classifier	A technology to effectively differentiate six forms of erythemato-squamous diseases using histopathological and clinical parameters of patients Improved quality of healthcare by accurately proffering diagnostic results to guide dermatologists in taking medical actions for the benefit of patients
[79]	IoT architecture based on ontology for deploying semantic IoT applications	Seamless environment for interoperability of heterogeneous vocabularies and data formats Sensorial observations are shared, data is contextualized, knowledge is reused, and information is processed to address integration and heterogeneity challenges of smart hospital system Improvements in healthcare delivery, business growth, and efficiency in diverse domains
[80–82]	Ambient assisted living (AAL). IoT architecture is based on Artificial intelligence	Monitoring activities, health, and behavior of incapacitated or elderly individuals in their homes using a convenient and safe approach

4 Future research trends of IoT-enabled healthcare infrastructure

The adoption of the IoT technology sector has witnessed a tremendous increase in the healthcare sector. It has been utilized extensively in the healthcare sector for monitoring the health status of patients. However, there is still enormous potential for transforming primary healthcare facilities and improving hospitals into a secondary care unit. Hence, it is imperative to ascertain potential technologies are that are feasible to address the challenges in achieving this goal.

Stroke and epileptic seizure predictions Research shows that a stroke is classified as one of the leading causes of untimely death across the globe [53, 54]. In addition, it estimates that 50 million people are deemed to be suffering from Epilepsy in the world. Therefore, predicting an epileptic seizure or a stroke in real-time is crucial in this research field. This can be achieved by developing machine learning (ML) algorithms that have the ability to detect and predict these incidents before they manifest. Thus, enabling quick response to counteract these incidents, as well as measures to prevent them. Therefore, integrating ML algorithms with IoT-enabled healthcare systems will improve the prediction accuracy of stroke and epileptic seizures in real time.

Prosthetics sensors Prosthetics built on the Tactile Internet communication are one of the major applications in healthcare [55, 56]. There is a necessity to implement a feasible sensor that can intelligently capture the events of an environment and filter out the redundant events (information) to obtain valuable information. Consequently, prosthetics is an important area for future research and implementation. These can be actualized by exploring algorithms that have the ability to extract valuable information from the data retrieved by the sensors.

Internet of nano things There are numerous flaws that are hindering the developmental stride of Internet of Nano Things (IoNT) for healthcare. For instance, the limited energy bank of IoNT. A potential energy harvesting technology can deliver possible solutions for a power-constrained IoNT network [57, 58]. In addition, design issues need to be resolved with respect to antenna design and there are flaws of interoperable protocols for interaction and the sharing of data. There is also the issue of signal interference within the body that needs to be rectified. Alternatively, IoNT can be deployed to develop an application of precision medicine in the future. For instance, nano-robots have the potential to deliver drugs to particular organs with a precise accuracy that leads to better treatment and a reduction in side-effects. Also, future development of communication standards that will improve the reliability of co-ordination and control of IoNT network needs consideration.

Precision in-vivo procedures The utilization of nano-robots deployed for the execution of complex in-vivo processes can be realized by using the TI [59, 60]. This application is mainly used to carryout remote surgery on patients that need additional functions which include the delivery of precision drugs and limited invasive processes in the future.

Blockchain Blockchains are gradually gaining relevance in IoT-enabled healthcare applications. The issues concerning security are a major set-back in developing a reliable IoT-enabled healthcare application [61–64]. However, blockchain technology have the ability to resolve the aforementioned challenges, due to its functionalities which comprise of the provisioning of secured data storage and authentication of devices.

5 Challenges in IoT-enabled healthcare application

The challenges facing IoT-based healthcare systems are broadly classified into two types, namely, infrastructural and security challenges as follows.

(A) ***Infrastructural challenges*** These challenges are further subcategorized and each one is summarized below.

(i) *Planning challenges*

The initiative of developing or adopting IoT-enabled systems to support healthcare infrastructure is often unsuccessful due to many challenges. Health centers and healthcare institutions may be persuaded to consider IoT technologies for rapid transmission of information. Definitely, there is a cause to be enthusiastic over prospects of IoT. Considering a study by Cisco [65], an exciting impression of IoT modification studies was described [66]. The study required obtaining responses from over 1800 individuals that were contributors in the past or pending IoT schemes across the UK, USA, and India. Regarding the Cisco study [65], completed projects were only considered as productive when it was 26% ahead of deadline.

This study did not focus on healthcare organizations; however, the healthcare industry was very much considered in the overall study. The findings emphasized that enterprises need to be careful when planning their IoT packages. For instance, considering their general business goals and patient demands, enterprises were encouraged to start small and organize their ideas.

(ii) *Generation of tremendous amount of data*

Approximately, all enthusiastic hospital administrations show concern for IoT initiatives to monitor people that walk around the hospital, monitor resources, provide efficient attention to medical instruments that may soon stop working, and reduce emergency room waiting period. These technological inventions are laudable; nonetheless, the huge amount of data collected are problematic for all of them. A forecast reveals that by 2025, the healthcare system will be responsible for generating large amounts of data in several sectors [67–69]. Hence, organizations must know that the decision to embrace IoT technology will probably require increased data storage. Additionally, according to guidelines, the health sector needs to be very careful about handling patient information through IoT devices. The enormous volume of information collected by the IoT devices utilized in healthcare may cause unexpected obstacles when institutions are not already prepared to establish its authenticity and manage it appropriately.

(iii) *IoT devices increase available attack*

The huge benefit of applying IoT devices in healthcare presents concerns about vulnerabilities. Because there is an increase in the use of devices, the numerous possibilities in the number of methods that hackers can explore to infiltrate the computer system and sabotage valuable data [70] are increasing. A study by uncovered a new threat. It indicated that by obtaining access to the network system and analyzing its error logs, hackers could master how a linked medical device worked. Using this knowledge, skilled hackers could break into the system of a selected hospital or make devices return altered measurements that may influence patient care. The study also shows some improvements in the readiness of manufacturers, suppliers, and vendors to cooperate. By overcoming the differences between sections of an IoT network, adapting dependable formalities, and strengthening standards, those shared cooperation can reduce risks for patients. It is impossible to understand all the security risks that healthcare institutions may face in the future. Establishments preparing to apply IoT technology should still consider the prevailing risks and understand how to fortify networks and devices from hackers.

(iv) *Outdated infrastructure hindering the medical industry*

The advantage of IoT is interesting if the infrastructure of a facility is good, functional, and not outdated. However, the presence of outdated facilities is a popular problem in hospitals and healthcare. When hospitals are deficient of updated facilities, they may have serious issues with employing the staff to make necessary advancements. Technology-savvy expertise is required and emerging healthcare organizations may not want to commence with outdated facilities.

(v) *IoT posing several overlooked obstacles*

Studies have shown that a patient monitoring system is the most frequently used IoT technology in clinics, hospitals, and healthcare institutions [71, 72]. It is certainly useful to agree with that system. One thing healthcare establishments often overlook is that contrary to websites, IoT devices usually cannot exceed the scheduled time for layoff. Rather, updates must continuously take place while people utilize the monitoring devices. Furthermore, hospitals consistently depend on IoT-enabled supply cabinets to locate materials. Once those networks are set up, the facilities can usually reduce hurdles in handling previous records. Moreover, because humans produce the IoT systems, even the most advanced devices cannot eliminate human error. This indicates that IoT systems can assume fallible performance from humans that produce them. Additionally, appraisals by vendors are important in overcoming usually unexpected problems.

Most producers are primarily bothered with surpassing market rivals with their products. Therefore, when consumer databanks are compromised, manufacturers should not be amazed because in the hustle of market competition, several manufacturers do not include security in their procedures from the beginning. Even if a hospital has typical cybersecurity protection, devices that do not have the necessary security may still pose threats to patients. One bad apple can spoil the barrel. Cybersecurity in the context of IoT-based healthcare must be uncompromising and complete. However, few IoT systems are secure in terms of traditional network security metrics.

(B) *Security challenges* Because IoT will be adopted by more businesses, there are new security challenges that will continuously be encountered, and this can be related to the limitations of the device. Moreover, when businesses embrace IoT, new security vulnerabilities will continue to emerge. The increased risk of security breaches may be attributed to device limitations. These security challenges include the following.

(i) *Rise of botnets*

There has been a recent increase in botnet attacks, which involve the infection of a network of computers by a malware controlled as a group while owners of IoT devices remain unaware. This problem occurs owing to the hacking of a device by malicious hackers that extract information for use in one illegal activity or another. A hospital is one of those organizations that can be affected by the botnet while management remains unaware of its occurrence [73]. This is because the organization does not have the required security to be able to track the botnet across its devices.

(ii) *Increased number of IoT devices*

Recently, cybersecurity experts have ensured the security of computers and mobile devices. Moreover, IoT is being increasingly adopted by both private and public organizations. Currently, approximately seven billion devices are being used and this number has a great tendency of reaching more than 20 billion before the year 2021. More IoT devices will lead to greater security vulnerabilities being affected by businesses, increasing the challenges of security experts.

(iii) *Need for encryption*

Encryption techniques, despite being an effective way of denying hackers access to information, are amongst the most important challenges for IoT security [74]. The devices used may not have storage and processing abilities possessed by traditional computers. This leads to an increase in the rate of attack, whereby hackers will readily manipulate the algorithms that are intended to provide safety and protection. Encryption can only be a security measure when this problem is solved.

(iv) *Outdated legacy security*

Interconnected legacy systems are also areas of concern. This is because the legacy technologies are usually outdated in enterprises with multiple IoT devices. A breach in a particular IoT device can lead to a breach of the interconnected legacy system that is lacking the appropriate security standards.

(v) *Weak default passwords*

Most IoT devices have default passwords that may not be strong. Although it is recommended that the passwords be reset, this is an instruction that is ignored by some information technology (IT) managers. When a password is weak or can easily be guessed, it increases the vulnerability of an IoT device to brute force attack. This problem is persistent in some countries and it requires immediate action. For instance, default passwords were banned in countries such as the United States of America.

(vi) *Unreliable threat detection methods*

There are numerous enterprises that are able to identify data breaching using either spotting indicators, monitoring the activities of users, or even using security protocols. These techniques were rendered ineffective, considering the increase in the population of IoT devices and device complexities.

(vii) *Small scale attacks in IoT*

Although experts in cybersecurity are being careful with large scales of attacks, the small attacks that are paid less attention to, can be threats on IoT. This is because they are more difficult to recognize and can occur without the knowledge of the organization. The hackers may operate through the main devices used by an organization such as printers, cameras, and scanners.

(viii) *Phishing attacks*

Phishing has already become a problem to cybersecurity in approximately all technologies used in organizations. However, IoT can be the vector of the latest attacks. Signals are usually sent by hackers to an IoT device that may result in a series of complications. Despite being among the commonly encountered attacks on cybersecurity, it is preventable if the organization can focus on providing awareness to their staff about the latest signs of phishing.

(ix) *Inability to predict threats*

Some organizations may not have a management system that is capable of monitoring activities and inspecting potential threats simultaneously, even though security experts were attempting to ensure an early prevention of attacks on IoT. If these proactive measures are not put in place, organizations will find it difficult to detect potential breaches at an early stage.

(x) *Infrequent updates*

One of the ways of ensuring security is for security professionals to regularly provide software updates. There are IoT devices that do not receive these updates. This may be received by other technologies and only some organizations attempt to provide significant security updates to IoT devices.

(xi) *IoT financial-related breaches*

Because organizations such as banking industries employ the use of IoT for electronic transactions, hackers have the tendency to attack the devices and make illegal transactions. Currently, organizations adopt machine learning or blockchain as a means of controlling financial fraud prior to its occurrence [75, 76]. Nonetheless, not every organization adopts this security measure.

(xii) *User privacy*

It is mandatory for enterprises to protect the data of both internal and external users. This is because of the use of IoT devices that are given by the organization to staff. Any breach in the privacy of an organization puts the reputation of that organization at risk; therefore, the security of IoT must be given the utmost priority. The security challenges of IoT are represented in Fig. 3.

Although the smart hospital management system provides the possibility of betterment of the quality of life of people because of its diverse application in a health-related system, it has a number of challenges. This requires an IoT architectural design that addresses the discussed challenges, and it must provide a system of communicating with these devices that is both manageable and interoperable.

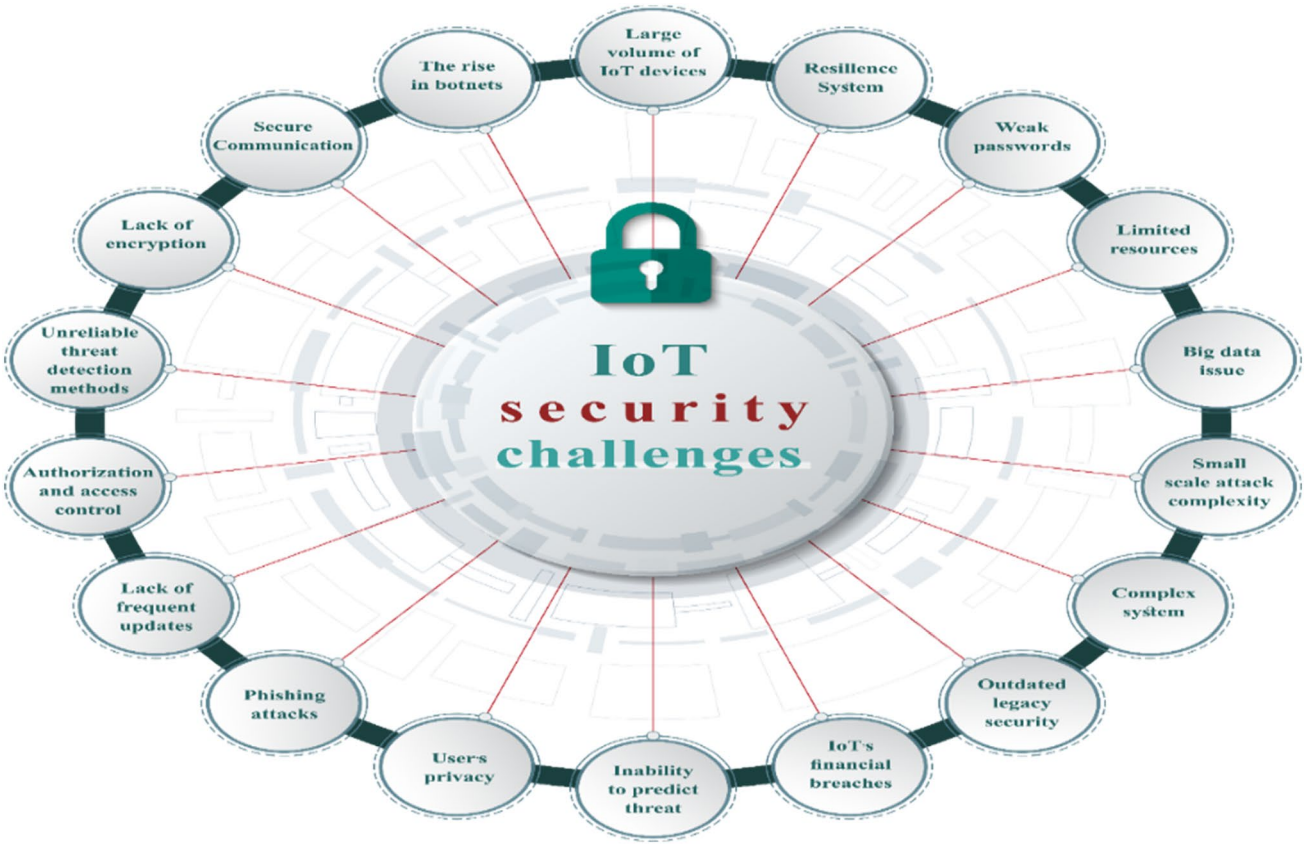

Fig. 3 Security problems in IoT

6 Conclusion

Health maintenance is one of the global challenges for humanity. In the last decade, the healthcare industry has attracted scholarly attention. This study investigates the current trends in the application of IoT technology in the healthcare sector and its potential benefits. Additionally, it investigates future trends which discuss emerging technologies that could improve the effectiveness and efficiency of IoT-enabled healthcare application for better treatment. Numerous challenges that tend to impede the development of reliable, effective, efficient, and scalable IoT-enabled healthcare applications as well as its adoption are highlighted and discussed extensively. Thus, opportunities that provide new insight and solutions for the improvement of quality health treatment that will enhance human life span. In the future, a re-enforcement algorithm will be developed and integrated in IoT-enabled healthcare infrastructure to resolve the challenges of redundant sensory data retrieved from wearable sensor devices.

Acknowledgements The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: (22UQU4320277DSR09).

Authors' contributions Supervision, project administration, conceptualization, methodology, investigation, resources, data curation, writing—original draft preparation, writing—review and editing, funding acquisition, the author has read and agreed to the published version of the manuscript.

Availability of data and materials There is no associated data or the data will not be deposited.

Declarations

Conflict of interest The author declares that there is no conflict of interests regarding the publication of this paper.

References

1. Figueroa CA, Harrison R, Chauhan A, Meyer L (2019) Priorities and challenges for health leadership and workforce management globally: a rapid review. BMC Health Serv Res 19(1):239
2. World Health Organization (2018) https://www.who.int/news-room/fact-sheets/detail/ageing-and-health. Accessed 18 Jan 2020
3. Ventola CL (2014) Mobile devices and apps for health care professionals: uses and benefits. Pharm Ther 39(5):356
4. Zhang Q, Lian B, Cao P, Sang Y, Huang W, Qi L (2020) Multi-source medical data integration and mining for healthcare services. IEEE Access 8:165010–165017
5. Devi MK, Vemuri VP, Arumugam M, UmaMaheswaran SK, Acharjee PB, Singh R, Kaliyaperumal K (2022) Design and implementation of advanced machine learning management and its impact on better healthcare services: a multiple regression analysis approach (MRAA). Comput Math Methods Med 2022:2489116
6. Aliyu A, Abdullah AH, Kaiwartya O, Cao Y, Lloret J, Aslam N, Joda UM (2018) Towards video streaming in IoT environments: vehicular communication perspective. Comput Commun 118:93–119
7. Doherty RF, Purtilo RB (2015) Ethical dimensions in the health professions-e-book. Elsevier Health Sciences, Amsterdam
8. Alturki R, Alharbi AI, AlQahtani SS, Khan S, Truong Hoang V (2021) A proposed application for controlling overweight and obesity within the framework of the internet of things. Mob Inf Syst. https://doi.org/10.1155/2021/7109099
9. Ranger S (2018) What is the IoT? Everything you need to know about the internet of things right now. ZDNet, January, 19
10. Baker SB, Xiang W, Atkinson I (2017) Internet of things for smart healthcare: technologies, challenges, and opportunities. IEEE Access 5:26521–26544
11. Dang LM, Piran M, Han D, Min K, Moon H (2019) A survey on internet of things and cloud computing for healthcare. Electronics 8(7):768
12. Esther OA, Jantan A, Abiodun OI, Arshad H, Dada KV, Emmanuel E (2020) HoneyDetails: a prototype for ensuring patient's information privacy and thwarting electronic health record threats based on decoys. Health Inform J 26:2083–2104
13. Colakovic A, Hadzialic M (2018) Internet of things (IoT): a review of enabling technologies, challenges and open research issues. Comput Netw 144:17–39
14. Akhigbe BI, Munir K, Akinade O, Akanbi L, Oyedele LO (2021) IoT technologies for livestock management: a review of present status, opportunities, and future trends. Big Data Cogn Comput (MDPI) 15(1):10–39
15. Manzoor A, Braeken A, Kanhere SS, Ylianttila M, Liyanage M (2021) Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain. J Netw Comput Appl 176:102917
16. Javed F, Afzal MK, Sharif M, Kim B-S (2018) Internet of things (IoT) operating systems support. Netw Technol Appl Chall Comp Rev IEEE Commun Surv Tutor 20(3):2062–2100
17. Pirmagomedov R, Koucheryavy Y (2021) IoT technologies for augmented human: a survey. Internet Things 14:100–120
18. Kumar A, Krishnamurthi R, Nayyar A, Sharma K, Grover V, Hossain E (2020) A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes. IEEE Access 8:118433–118471
19. Vo DT, Nguyen XP, Nguyen T, Hidayat R, Huyhn TT, Nguyen DT (2021) A review on the internet of things (IoT) technologies in controlling ocean environment. Energy Sources Part A Recov Util Environ Eff 43(24):323–346
20. Gomez-Chabla R, Real-Aviles K, Moran C, Grigalva P, Recalde T (2019) IoT applications in agriculture: a systematic literature review. In: ICT for agriculture and environment, Springer, p 68–76
21. Abualigah L, Zitar RA, Almotairi KH, Hussein AM, Abd Elaziz M, Nikoo MR, Gandomi AH (2022) Wind, solar, and photovoltaic renewable energy systems with and without energy storage optimization: a survey of advanced machine learning and deep learning techniques. Energies 15(2):578
22. Ahmadi H, Arji G, Shahmoradi L, Safdari R, Nilashi M, Alizadeh M (2019) The application of internet of things in healthcare: a systematic literature review and classification. Univ Access Inf Soc 18(4):837–869
23. Mukherjee S, Biswas GP (2018) Networking for IoT and applications using existing communication technology. Egypt Inform J 19(2):107–127
24. Chanak P, Banerjee I (2020) Internet-of-things-enabled smart-villages: an overview. IEEE Consum Electron Mag 10(3):12–18
25. Catarinucci L, De Donno D, Mainetti L, Palano L, Patrono L, Stefanizzi ML, Tarricone L (2015) An IoT-aware architecture for smart healthcare systems. IEEE Internet Things J 2(6):515–526
26. Ghazal TM, Hasan MK, Alshurideh MT, Alzoubi HM, Ahmad M, Akbar SS et al (2021) IoT for smart cities: machine learning approaches in smart healthcare—a review. Future Internet 13(8):218
27. Dash S, Shakyawar SK, Sharma M, Kaushik S (2019) Big data in healthcare: management, analysis and future prospects. J Big Data 6(1):54
28. Zeadally S, Siddiqui F, Baig Z, Ibrahim A (2019) Smart healthcare: challenges and potential solutions using internet of things (IoT) and big data analytics. PSU Res Rev 1–17
29. Abujayyab SK, Almotairi KH, Alswaitti M, Amr SSA, Alkarkhi AF, Taşoğlu E, Hussein AM (2021) Effects of meteorological parameters on surface water loss in Burdur Lake, Turkey over 34 years Landsat Google earth engine time-series. Land 10(12):1301
30. Otair M, Alhmoud A, Jia H, Altalhi M, Hussein AM, Abualigah L (2022) Optimized task scheduling in cloud computing using improved multi-verse optimizer. Clust Comput. https://doi.org/10.1007/s10586-022-03650-y
31. Dhanvijay MM, Patil SC (2019) Internet of things: a survey of enabling technologies in healthcare and its applications. Comput Netw 153:113–131
32. Kelly JT, Campbell KL, Gong E, Scuffham P (2020) The Internet of Things: Impact and implications for health care delivery. J Med Internet Res 22(11):e20135
33. Thamara A, Elsersy M, Sherif A, Hassan H, Abdelsalam O, Almotairi KH (2021) A novel classification of machine learning applications in healthcare. In: 2021 3rd IEEE Middle East and North Africa COMMunications conference (MENACOMM), IEEE, p 80–85
34. Tian S, Yang W, Le Grange JM, Wang P, Huang W, Ye Z (2019) Smart healthcare: making medical care more intelligent. Glob Health J 3:62–65
35. Birje MN, Hanji SS (2020) Internet of things based distributed healthcare systems: a review. J Data Inf Manag 2(3):149–165
36. Cook DJ, Duncan G, Sprint G, Fritz RL (2018) Using smart city technology to make healthcare smarter. Proc IEEE 106(4):708–722
37. Ijemaru GK, Ang LM, Seng KP (2022) Transformation from IoT to IoV for waste management in smart cities. J Netw Comput Appl 204:103393
38. Ratta P, Kaur A, Sharma S, Shabaz M, Dhiman G (2021) Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives. J Food Qual 2021
39. Zamanifar A, Nazemi E (2019) An approach for predicting health status in IoT health care. J Netw Comput Appl 134:100–113

40. Zeadally S, Bello O (2021) Harnessing the power of Internet of Things based connectivity to improve healthcare. Internet Things 14:100074
41. Vatandoost M, Litkouhi S (2019) The future of healthcare facilities: how technology and medical advances may shape hospitals of the future. Hosp Pract Res 4(1):1–11
42. Atawneh SH, Ghaleb OAM, Hussein AM, Al-Madi M, Shehabat B (2020) A time series forecasting for the cumulative confirmed and critical cases of the covid-19 pandemic in Saudi Arabia using autoregressive integrated moving average (ARIMA) model. J Comput Sci 16:1278–1290
43. Yogaraj A, Ezilarasan MR, Anuroop RV, Sivanthiram CS, Thakur SK (2017) IOT based smart healthcare monitoring system for rural/isolated areas. Int J Pure Appl Math 114(12):679–688
44. Balandina E, Balandin S, Koucheryavy Y, Mouromtsev D (2015) IoT use cases in healthcare and tourism. In: 2015 IEEE 17th conference on business informatics, vol 2. IEEE, p 37–44
45. Laplante PA, Laplante N (2016) The internet of things in healthcare: potential applications and challenges. IT Prof 18(3):2–4
46. Alshamrani M (2021) IoT and artificial intelligence implementations for remote healthcare monitoring systems: a survey. J King Saud Univ Comput Inf Sci 34:4687–4701
47. Kulkarni A, Sathe S (2014) Healthcare applications of the internet of things: a review. Int J Comput Sci Inf Technol 5(5):6229–6232
48. Distefano S, Bruneo D, Longo F, Merlino G, Puliafito A (2016) Hospitalized patient monitoring and early treatment using IoT and cloud. BioNanoScience 7(2):1–4
49. Moser LE, Melliar-Smith P (eds) (2015) Personal health monitoring using a smartphone. In: Mobile services (MS), 2015 IEEE international conference on IEEE
50. Uckelmann D, Harrison M, Michahelles F (2011) An architectural approach towards the future internet of things. In: Uckelmann D, Harrison M, Michahelles F (eds) Architecting the internet of things. Springer, Berlin, pp 1–24
51. Segura AS, Thiesse F, Winkelmann A (2016) The internet of things: business applications, technology acceptance, and future prospects. Dissertation, University of Würzburg
52. Ubale Kiru M, Belaton B, Chew X, Almotairi KH, Hussein AM, Aminu M (2022) Comparative analysis of some selected generative adversarial network models for image augmentation: a case study of COVID-19 X-ray and CT images. J Intell Fuzzy Syst 1–20 (**preprint**)
53. Daoud H, Williams P, Bayoumi M (2020) IoT based efficient epileptic seizure prediction system using deep learning. In: 2020 IEEE 6th world forum on internet of things (WF-IoT), IEEE, p 1–6
54. Zhang S, Chen D, Ranjan R, Ke H, Tang Y, Zomaya AY (2021) A lightweight solution to epileptic seizure prediction based on EEG synchronization measurement. J Supercomput 77(4):3914–3932
55. Qadri YA, Nauman A, Zikria YB, Vasilakos AV, Kim SW (2020) The future of healthcare internet of things: a survey of emerging technologies. IEEE Commun Surv Tutor 22(2):1121–1167
56. Stolyarov R, Carney M, Herr H (2020) Accurate heuristic terrain prediction in powered lower-limb prostheses using onboard sensors. IEEE Trans Biomed Eng 68(2):384–392
57. Akkaş MA, Sokullu R, Cetin HE (2020) Healthcare and patient monitoring using IoT. Internet Things 11:100173
58. Strobel G, Mittnacht J (2021) Richard, are we there yet?—An internet of nano things information system architecture. In: Proceedings of the 54th Hawaii international conference on system sciences, p 4578
59. Banerjee A, Chakraborty C, Rathi M Sr (2020) Medical imaging, artificial intelligence, internet of things, wearable devices in terahertz healthcare technologies. Terahertz biomedical and healthcare technologies. Elsevier, Amsterdam, pp 145–165
60. Fabelo H, Halicek M, Ortega S, Shahedi M, Szolna A, Piñeiro JF, Sosa C, O'Shanahan AJ, Bisshopp S, Espino C, Márquez M (2019) Deep learning-based framework for in vivo identification of glioblastoma tumor using hyperspectral images of human brain. Sensors 19(4):920
61. Conti M, Kumar G, Nerurkar P, Saha R, Vigneri L (2022) A survey on security challenges and solutions in the IOTA. J Netw Comput Appl 203:103383
62. Satamraju KP (2020) Proof of concept of scalable integration of internet of things and blockchain in healthcare. Sensors 20(5):1389
63. Srivastava G, Parizi RM, Dehghantanha A (2020) The future of blockchain technology in healthcare internet of things security. In: Blockchain cybersecurity, trust and privacy, p 161–184
64. Yousefnezhad N, Malhi A, Främling K (2020) Security in product lifecycle of IoT devices: a survey. J Netw Comput Appl 171:102779
65. Cisco (2019) Cisco survey reveals close to 3/4ths of IoT projects are failing | the network. [Online]. Available: https://newsroom.cisco.com/press-releasecontent?type=webcontent&articleId=1847422. Accessed 21 Mar 2019
66. Aleström F, Almgren E (2019) Metodik för utveckling av Proof of Concept inom Internet of Things: XPD (eXtreme PoC Development) en ny projektmetodik som säkrar affärsnyttan i utvecklingen av IoT-lösningar
67. Alotaibi M, Alotaibi SS (2022) Optimal disease diagnosis in internet of things (IoT) based healthcare system using energy efficient clustering. Appl Sci 12(8):3804
68. Raghupathi W, Raghupathi V (2014) Big data analytics in healthcare: promise and potential. Health Inf Sci Syst 2(1):3
69. Vogenberg FR, Santilli J (2018) Healthcare trends for 2018. Am Health Drug Benef 11(1):48
70. Zittrain J (2008) The future of the internet—and how to stop it. Yale University Press, London
71. Dauwed M, Meri A (2019) IOT service utilization in healthcare. In: IoT and smart home automation. IntechOpen, Rijeka
72. Madakam S, Lake V, Lake V, Lake V (2015) Internet of things (IoT): a literature review. Comput Commun 3(05):164
73. Javed SH, Ahmad MB, Asif M, Almotiri SH, Masood K, Ghamdi MAA (2022) An intelligent system to detect advanced persistent threats in industrial internet of things (I-IoT). Electronics 11(5):742
74. Abunadi I, Abdullah Mengash H, Alotaibi S, Asiri MM, Ahmed Hamza M, Zamani AS, Motwakel A, Yaseen I (2022) Optimal multikey homomorphic encryption with steganography approach for multimedia security in internet of everything environment. Appl Sci 12(8):4026
75. Auer S, Nagler S, Mazumdar S, Mukkamala RR (2022) Towards blockchain-IoT based shared mobility: car-sharing and leasing as a case study. J Netw Comput Appl 200:103316
76. Kamal M, Aljohani AJ, Alanazi E, Albogamy FR (2022) 5G and Blockchain enabled lightweight solutions for containing COVID-19. Secur Commun Netw 2022:1–12
77. Banu SM, Dascălu LM, Toacşe G (2013) Internet of things in psoriasis assessment and treatment. In: Doctoral conference on computing, electrical and industrial systems, pp 172–179. Springer, Berlin
78. Güvenir HA, Emeksiz N (2020) An expert system for the differential diagnosis of erythemato-squamous diseases. Expert Syst Appl 18(1):43–49
79. Zgheib R (2017) SeMoM, a semantic middleware for IoT healthcare applications, doctoral dissertation
80. Blackman S, Matlo C, Bobrovitskiy C, Waldoch A, Fang ML, Jackson P, Sixsmith A (2016) Ambient assisted living technologies for aging well: a scoping review. Int J Intell Syst 25(1):55–69

81. Fleury A, Vacher M, Noury N (2009) SVM-based multimodal classification of activities of daily living in health smart homes: sensors, algorithms, and first experimental results. Trans Inf Technol Biomed 14(2):274–283
82. Noury N, Hervé T, Rialle V, Virone G, Mercier E, Morey G, Porcheron T (2000) Monitoring behavior in home using a smart fall sensor and position sensors. In: 1st Annual international IEEE-EMBS special topic conference on microtechnologies in medicine and biology. Proceedings (Cat. No. 00EX451), IEEE, p 607–610