Defining the Scope of the Internet of Things with a Particular Focus on Its Role in Healthcare: A Review Paper

Abdulaziz Alomari [1†] and Ben Soh [2††],

Department of Computer Science and IT, La Trobe University, Bundoora, Vic, 3086, Australia

Abstract
Today's world is experiencing rapid technological advancement like never before. The ever-changing technology space has overwhelmed citizens with a substantial load of information, which has made it difficult for them to keep up with the technology awareness. This review paper is written to provide information about the Internet of Things in a way that technical along with non-technical individuals can understand the definition, historical evolution, components, and scope of IoT technology. Relevant literature published between January 2009 and February 2023 was included in this paper. The applications of the Internet of Things in healthcare have been a special focus of this paper as IoT has massive potential in this field and healthcare professionals often face significant issues in keeping their technology knowledge up to date. Moreover, some of the most common issues associated with IoT introduction in healthcare are also discussed in the paper along with some suitable recommendations. Although, IoT can significantly transform our lives and can introduce convenience and efficiency, particularly in the healthcare sector. However, its adoption in healthcare is still a major task due to various challenges presented by the health workforce. Thus, in-depth empirical research is suggested to assist the IoT technology transition.

Keywords:
Internet of Things, Technology education, Digital health, IoT use in healthcare.

1. Introduction

The 21st century is an era of rapid technological development, and the introduction of advanced technologies has constantly been redefining societies' functioning and future. It is expected that digital technologies will revolutionise conventional procedures and will provide solutions that have never been thought of before. Similarly, the healthcare industry is at the forefront of technological advancement due to rising costs and increasing workloads on healthcare organisations and clinicians [1]. However, the adoption of new technologies, such as the Internet of Things has not been smooth in the healthcare sector due to various challenges presented by healthcare professionals [2]. Thus, this paper is developed to provide detailed information about the evolution, components and uses of the Internet of Things to support the understanding of non-technical users, particularly healthcare professionals, about this new technology.

2. Background - Internet of Things or IoT

The Internet of Things (IoT) is a significant development in the field of information technology. Broadly, it refers to the connection of devices, such as everyday use objects or appliances to the internet and allowing them to send and receive data. The phrase "Internet of Things" is made up of two words "Internet" and "Things" [3]. The Internet is a global network of interconnected computers which serve users around the world. According to Statistics (2022) [4], as of April 2022, there were more than five billion Internet users worldwide, representing 63.1% of the world's population. The percentage of internet users has almost doubled in the last decade, and it is increasing at a fast rate, which not only illustrates the technological acceptance of individuals but also depicts technological dependence [5,3].

However, the world order has not always been like this, it was only a few decades ago when scientists discovered the internet. Figure 1 illustrates the evolution of IoT and shows that almost four decades ago, in the pre-internet phase, communication was mainly conducted through the telephone line [6,7]. Then with the advent of the internet, mobile and email dominated communication mediums and this phase was called the 'Internet of Content' phase, where information was exchanged in the form of texts as well as visuals [6,7]. Following that, the 'Internet of Services' phase came along, where E-commerce becomes a major part of internet. Following that the fourth - the 'Internet of People', phase dominated, and people started communicating through social media applications such as Skype, Instagram, Facebook, etc. In the current time, the large-scale autonomous

Manuscript received April 5, 2023
Manuscript revised April 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.4.25

connections have started between electronic devices which support independent communication through the internet, and this phase is called the IoT and lately, these interconnected electronic devices have started to conduct independent decision making using artificial intelligence (AI) incorporation [7].

Figure 1: Evolution of IoT

The term “Internet of Things” (IoT) was coined by Kevin Ashton in 1999, who was a British technology pioneer and worked at the Massachusetts Institute of Technology [8,9]. In 2009 Kevin Ashton said that "I could be wrong, but I'm fairly sure the phrase "Internet of Things" started life as the title of a presentation I made at Procter & Gamble (P&G) in 1999. Linking the new idea of RFID in P&G's supply chain to the then-red-hot topic of the Internet was more than just a way to get executive attention. It summed up an important insight which is still often misunderstood." [9]. Although, in today’s world IoT has been called different names and concepts such as Machine-to-Machine Interaction, Web of Things, Pervasive Computing, etc. [3,10]. Even some tech giants like Cisco and Intel have used the term ‘Internet of Everything’ and embedded ‘Everything’ instead of ‘Things’ [10].

However, all these terms refer to the connectivity in everyday objects and the integration of computation that can increase the invisibility of technology in our lives and communication between devices without human intervention [3]. It is important to note that, despite advancements in technological awareness, the term IoT and other related terms are not widely understood by regular internet users [11]. One of the popular knowledge crowdsource websites, Quora, shows that the question “what is Internet of Things (IoT)?” or a similar question has been viewed over 100,000 times, which demonstrates the popularity trend of IoT and the aptitude of individuals towards its understanding [12].

As suggested above, IoT includes different components such as smart devices or machines that communicate with each other, gather information, and make decisions without human intervention [13]. Smart devices are a crucial part of this network as these devices use communication protocols to transmit collected data through sensors, which are then stored in a cloud infrastructure for processing. As shown in figure 2, the ecosystem of IoT includes smart devices, communication protocols, and cloud structures for data storage and analysis [13]. Processing, storing, and analysing the data in the cloud is important, and machine learning or AI methods are often used for this purpose [14].

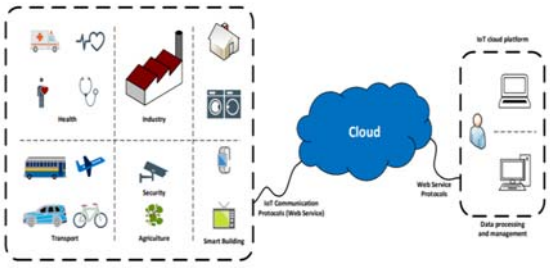

Figure 2: Core components of IoT [14].

3. IoT Layers

The three core components of IoT are also often classified into three layers: the perception layer, the network layer and the application layer (Figure 3) [15]. The perception layer is the physical layer and consists of sensors that gather information about the environment [15]. The network layer is responsible for connecting smart devices, network devices, and servers and transmitting and processing sensor data [15]. The application layer delivers application-specific services to the end user and specifies various areas where IoT can be utilized, such as smart industries, smart cities, smart health etc [15]. The sensor layer or perception layer is similar to human receptors such as eyes or ears and is responsible for gathering information from the environment through various sensors. These sensors include but are not limited to temperature, humidity, movement and vibration sensors and are used to detect and collect data about different aspects of the environment. The specific sensors chosen for a particular application will depend on the specific needs and goals of the system [16].

The network layer is responsible for transmitting data between the perception and application layers. This layer uses various communication technologies, such as cellular networks, satellite, WiFi, Bluetooth,

and low-power wide-area networks (LPWAN), to transmit data from physical objects. The data can be transmitted wirelessly or through a wired connection, such as via a gateway/router or via ethernet directly to the internet [3,14]. The application layer is responsible for the operation and management of all applications within a system. It provides services to these applications and processes the data received from the network layer [14]. The processing of this data can range from simple checks, such as verifying that a temperature reading is within a certain range, to more complex tasks, such as using computer vision to identify objects in video footage which may incorporate AI [17]. These results are then shown to the user on some sort of interface, where meaningful data is presented to assist user in decision making [17].

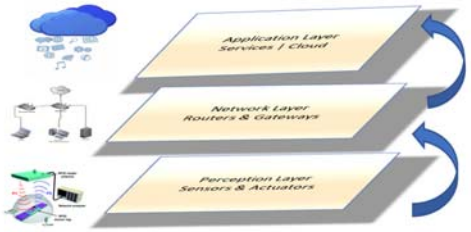

Figure 3: Three layers of IoT

4. Artificial Intelligence or AI

The capacity to incorporate AI in IoT is the primary factor that makes this technology substantially different from other technologies. Artificial intelligence or AI is the most recent invention of computer science aimed at creating machines that can accomplish tasks that conventionally require human assistance or mainly human intelligence ([18,19]. These tasks may include but are not limited to solving complex problems, making independent decisions, learning autonomously and adapting to new situations. Further, it is only fair to suggest that AI is different to human brain in some ways but better in most ways. For instance, human intelligence holds the ability to make creative and innovative decisions, while AI systems are designed to choose the most appropriate decision based on the available data and algorithms. Similarly, AI systems are highly effective in reducing the repetition of tasks and improving efficiency, as they can process and analyse data faster than humans and operate around the clock without the need for a break or rest [18]. Overall, the development of AI has the potential to significantly impact how humans work and live by automating many routine tasks and freeing humans to focus on more complex and creative work [18]. However, it also indicates a direct threat to working-class individuals in society, including those who are involved in repetitive work or work that is based on standard protocols, which can be replaced by AI or IoT incorporating AI [19].

5. Methodology

Relevant literature published between January 2009 and February 2023 in peer-reviewed journals and reliable websites was included in this research. Since the topic of the paper is relatively novel, special consideration was given to source and include up-to-date knowledge in this paper.

6. Overview of IoT Applications Around the Globe

IoT has multidisciplinary applications in the world, which range from environmental applications to transportation and infrastructure, agricultural, industrial and health [17,20]. Figure 4 shows some of the vital applications of IoT in critical sectors of the world. Smart city is one of the trendy IoT application areas, which include smart homes, streets, commercial markets and other structural and functional components of the cities [20]. IoT-enabled smart homes include home appliances such as television, home heating and colling systems, security systems and other audio/video streaming devices, all connected to work independently and efficiently [20,21].

The application of IoT in smart cities not only provides comfort to the users but also assists house owners in reducing energy costs, which may have much broader beneficial impacts on the environment [22]. Similarly, modern cars are equipped with smart intelligent sensors and devices that can control most components of cars ranging from headlights to the engine. The IoT is planned to integrate new systems in the car which can create wireless communication between car to car, car to driver and car to home to provide predictive maintenance and safe and comfortable driving experience [20].

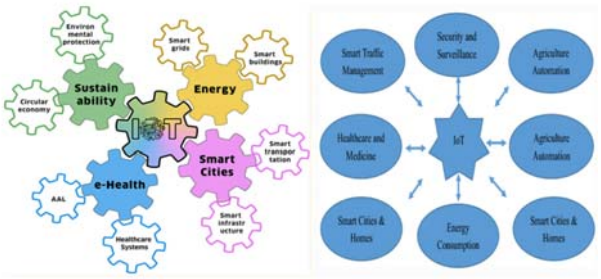

Figure 4: Domain of IoT [17,20]

Interestingly, Saudi Arabia has become the world leader in the smart city concept as Prince Mohammed Bin Salman has approved the world's first-ever Line City [23]. The Line City is based on the concept of no roads, cars or emissions and is planned to run 100% renewable, with 95% of the land being preserved for nature. The city is planned to be built in the desert of Tabuk on a straight line which will be 170 kilometres long and 200 metres wide. However, despite the fact the city is being built on just 34 square kilometres of land, it is predicted that it can accommodate around 9 million people.

Through IoT and smart devices, the Line City will have an ideal climate all year long and the residents will have access to all amenities within a five-minute walk [23]. Moreover, it is essential to highlight that Line City is not a concept anymore, the work on the city has already been started and it is planned to complete its initial phase by 2024 [24,23]. There is no precedent like Line City in the world and Prince Mohammed Bin Salman and Saudi Arabia have shocked the world by becoming the world leader in the smart city concept.

7. Uses of IoT in Healthcare

The list of applications of IoT in the health sector has become endless with the rapid evolution of the healthcare ecosystem in this modern century. In contrast to the past, the current healthcare system has advanced in a myriad of domains which includes but not limited to personalised healthcare, facilities provided in the healthcare buildings, robotics, smart beds and biosensors, the pharmaceutical industry and smart pills, remote patient monitoring and various other healthcare specialisations and treatments of diseases. Considering the immense magnitude of the topic, the following section will include a discussion on some of the most significant uses of IoT in the health sector.

7.1 Key Benefits of IoT

The uses and benefits of IoT in different healthcare sectors are discussed in the below section. Here are some major advantages of IoT incorporation in healthcare.

- IoT can reduce healthcare costs by reducing unnecessary hospital visits, reducing load on clinicians and remote patient monitoring, diagnosis, and care [1].
- IoT can improve treatment outcomes by supporting the early detection of diseases, supporting analysis and increasing accuracy in collected data [25].
- IoT can reduce medical errors as it will reduce clinicians' fatigue and collect detailed and precise data automatically free of human error [26,27].
- Last but not least, the inclusion of the above benefits will increase patient compliance and satisfaction and the overall quality of healthcare [28].

7.2 Remote Patient Monitoring

One of the significant benefits of IoT for patients and physicians is its capability to monitor different physiological biomarkers and conditions which can assist in disease management and prevention. This feature can not only assist clinicians in diagnosis and prevention but can also reduce workload in the busy healthcare environment.

The report provided by World Health Organization (WHO) on disabilities and aging suggests that the average life expectancy has improved substantially in the last few decades and as per the current pattern, it is likely that majority of the people worldwide will live beyond 60 years age mark [29]. While on the one hand, this increase in average life illustrates the success of medical science, but on the other, it also demonstrates an increase in the likelihood of aging issues such as chronic diseases, disabilities, and higher hospitalization rates [30]. According to healthcare researchers, healthcare services delivery is currently undergoing a transformation into a balance between hospital and home, which will majorly shift towards home-care health services by the year 2030 [31]. This healthcare services delivery revolution

encompasses all major features of patient disease prevention, identification, management and cure such as constant monitoring of vital signs through wearable devices, management of the emergency situation, rehabilitation strategies, medication management, telemedicine and much more [32].

IoT-based home healthcare solutions are one of the most effective solutions to overcome the health issues associated with the increase in the elderly population [29]. Home monitoring of patients or individuals at risk of serious health issues is a crucial application of Wireless Sensor Networks (WSN), where a combination of sensors are installed at patient's home that can track their activities. Moreover, the inclusion of smart objects such as video-based technology, RFID and near-field communication (NFC) by connecting different smart devices can lead to fast and effective communication between patients, objects and clinicians and objects themselves, which can facilitate monitoring processes in the home healthcare [29].

Similarly, remote ECG monitoring using IoT sensors has huge potential to detect and alarm healthcare providers about critical heart conditions at an early stage of disease [33,34,35]. In remote ECG monitoring, the patient can attach sensors to the body as a wearable device that can record the electrical activity of a heart and supply information about heart rate and rhythm. This information can assist clinicians in predicting various conditions such as heart enlargement, high Blood pressure, heart attack, etc [34,35]. One recent study by [36] demonstrated the real-life application of IoT sensors and machine learning for diagnosing heart conditions. The study findings showed an accuracy of 96%, a precision of 90%, and sensitivity and specificity of 80% and 73%, respectively, suggesting the high value of this kind of application for clinicians [36].

7.3 Improved Medication Adherence

One of the most substantial issues in healthcare includes medication errors, including inadequate prescribing, non-adherence or compliance to medication and inadequate monitoring of drugs, all of which can lead to various health issues and or even can cause death. The research conducted by [37] in 64 Norwegian hospitals reported 3372 medication errors in a period of just one year. The primary errors reported by the study were related to dosing of drugs (38%), complete omissions (23%) and incorrect drug (15%). Similarly, it has been suggested that yearly 9.5% of all deaths are linked to medical errors in the United States of America [38]. However, research indicates that the effective use of IoT technology can immensely assist in reducing medication errors.

The study by [39] explored the inclusion of a smart wearable device for medication reminders by creating a mobile application for android-based watches which can remind patients about the time and dose of the medicines. The issue of missing a medicine dose is also a critical medication error in hospitals as indicated by [40]. Baqir et al. (2015) [40] noted that to reduce this issue, the hospital pharmacy assistants had to make an extra effort by accompanying nurses on ward rounds. To resolve this, Serdaroglu et al. (2015) [41] built a medication adherence technique that employed different RFID for different medication types, multiple sensors and a notification system for mobile phones. The system was designed to ensure that patients were given the right medicine at the recommended time. Moreover, the wrong medication warning feature to the physicians was also included in the system to reduce medication side effects and serious health issues [41].

7.4 Early Disease Detection

The first step in early disease detection is the recognition of initial disease symptoms [42]. However, the mere recognition of disease symptoms is not enough to conduct the differential diagnosis [42]. In a real-life health setting, physicians are equipped with in-depth medical knowledge and training and thus, they can diagnose diseases adequately. In order to efficiently alarm clinicians about the occurrence of any new disease, IoT technology, smart devices and sensors require not only the collection of a large amount of data but also constant communication with the wireless cloud network [43]. The wireless cloud network can store and analyse the data to conduct the diagnosis based on knowledge taken from medical references and books and pre-set protocols for diagnosis defined and trained by the clinicians. Based on that, a relevant alert can be generated to the ambulance, doctors, caregivers, or the central health department of the country. This system can assist in diagnosis at an early stage, which can positively affect disease outcomes. In the past years, several IoT cloud-based platforms have been developed to prevent and control viral diseases [43].

The study by Sareen et al. (2017) [44] provided an IoT-based framework to prevent and manage a viral infection called the Zika virus. In the first step of the framework, the user is required to enter their identifiable information in the smart application (Android or IOS), upon which a unique identification number is generated for every single user. Following that, the user completes a series of questions that are based on the symptoms of the disease and only contain the 'Yes' and 'No' options to generate the user's unique attribute. After that, the automated analysis is conducted using a Naïve Bayesian Network algorithm to classify the user as infected or uninfected [44].

In the second step, a tracking system is activated via wireless mosquito sensors and Google maps using the Geographic Positioning System (GPS). These sensors are used to track the mosquito-dense site location, mosquito breeding site location, area temperature and humidity [44]. The tracked locations are then provided to the uninfected users to assist them with the path away from the critical locations. The high-risk location coordinates are sent to the healthcare department and other government agencies so adequate measures can be taken to stop the spread. The researchers tested the framework with the datasets of 2 million actual users and collaborated their demographic and symptom information to generate the results. The researchers concluded that the system provided high accuracy for initial diagnosis (based on the reported symptoms and cloud analysis) and for identifying high-risk areas using GPS [44].

7.5 IoT and COVID-19 Epidemic

Considering the current global epidemic of COVID-19, many researchers have proposed various IoT-based solutions to prevent future outbreaks [45]. The inclusion of AI in IoT has the capability to solve the issue of COVID-19 if applied adequately [46]. Furthermore, the IoT and AI can assist in monitoring and forecasting the disease, assist in the disease management process, allow researchers to virtually conduct simulation studies on the virus, and even help stop fake news related to COVID-19 [46]. The key to combat COVID-19 or any other viral/bacterial outbreak is to detect and diagnose the disease at its early stages so the spread can be hampered [45]. For instance, the massive global epidemic might have been avoided if COVID-19 had been detected and diagnosed in the early stages when the infection was limited to Wuhan, China. Early detection can assist healthcare providers in incorporating measures to restrict the infection and develop treatment plans than can save millions of lives and stop the spread [47].

Similar to the Zika virus, the first step in the initial diagnosis of COVID-19 is an adequate understanding of the symptoms of disease. According to the CDC (2020) [47], COVID-19 includes a wide array of symptoms which include but are not limited to cough, fever or chills, shortness of breath, fatigue, body pain, runny nose, loss of taste or smell, nausea or vomiting, sore throat and diarrhea. Moreover, among these, fever or chills is one of the most commonly reported symptoms of COVID-19 [47]. IoT infrastructure has the potential to conduct the disease detection process much faster and collect data more efficiently with the use of sensors and smart devices. This data can be shared with clinicians, other healthcare providers, and relevant authorities to control or stop this rapidly spreading disease [48]. Different smart devices can be included in the IoT framework to conduct the aforementioned process and detect COVID-19 at an early stage. Smart thermometers such as iFever, Tempdrop and Ran's Night can be included, which can sense body temperature and report to the smartphone app 24/7. There are many instances when patients are unaware of the initial change in body temperature; these devices can be used among high-risk patients to conduct 24/7 disease monitoring [45]. Another smart wearable device known as smart helmet has shown more safety and efficacy than the infrared thermometer gun due to the use of thermal cameras that can limit human interaction [49].

The smart helmet can detect abnormal body temperature along with the location and image of the patient taken through the optical camera. This information is then sent to the health officer via an alarm on the mobile phone so that authorities can take relevant measures [50]. Moreover, similar to the Zika virus protocol, GPS location can be added via Google maps to locate the places visited by the patient after the detection [51]. Countries such as China, Italy and UAE have implemented this wearable device and model has shown an accuracy of 96 percent for the detection of high body temperature [52]. Identification of COVID-19 infected individuals is also important in the crowd to control its spread [53]. Drone technology, such as Unmanned Aerial Vehicles (UAV) incorporating IoT can be used to fast-track the process of finding contaminated people and identifying high-

risk zones during the pandemic. Drones can capture and screen a large number of people in a crowd at once and can even reach places that are not readily reachable by the usual screening personnel with a thermometer gun [54]. A Canadian company has introduced this technology and uses drone cameras to detect temperature, cough, sneeze and heart rate in large crowds [55].

8. Potential Issues with IoT in Healthcare

Despite of above-mentioned advantages, according to Al-Rawashdeh et al. (2022) [2], who conducted a recent systematic review on IoT adoption, the inclusion and acceptance of IoT in healthcare is still low. They suggested that the healthcare workforce present significant challenges in the adequate implementation of IoT-based systems. These factors vary from technological to individual, environmental to social and require special consideration and in-depth research as they may vary from region to region and population to population [2]. A brief overview of the IoT issues is provided below that can impact the acceptance behaviour of healthcare professionals, to highlight the complexity of the subject.

8.1 Data Security and Privacy Issues

While issues with data security are not new in the context of information technology, the characteristics of the IoT platforms present unique and novel data security challenges. Inadequately secured IoT-based devices and applications can provide an open path for a cyber-attack and expose user personal information at risk of theft [56]. The interconnected aspect of the IoT platform implies that every device which is inadequately secured and linked to the Internet has the potential to provide a gateway and compromise the integrity of the whole system. This challenge is further enhanced by the widespread implementation of identical IoT-based devices and the capability of these devices to connect without requiring permission from the user [57]. Moreover, the large number of gadgets installed in the healthcare or hospital environment also provides an opportunity to hackers to access the systems that store private and personal information of the patients and staff [58].

It is well-known by hackers that medical gadgets do not store patient data. However, they use these as an entry point into the system. In IoT infrastructure majority of these devices will be linked to each other and the central system. These medical gadgets lack the security present on other devices, such as desktops, laptops and cloud networks and that is why they are regarded as an easy target [58]. Similarly, the nature of the information stored in the IoT networks installed in healthcare settings makes it more vulnerable to the attack of hackers. According to Perwej et al. (2022) [58], medical information is ten times more worthy for hackers than credit card numbers. According to estimates provided by the IBM study on security, the average data breach in the year 2020 was estimated at $3.86 million across all global businesses, while healthcare incurred a cost of around $7.13 million, which was the highest among all industries [59].

Similarly, the inclusion of mobile phones in the IoT networks as interface device to receive notification and analysis reports on various android and IOS app also increase the threat of data theft [58]. When the healthcare organisation allows mobile logins, security quality is compromised as the organisation's security does not affect the communication devices of the employees, leaving room for exposure to hackers and malware. The use of personal communication devices is important in healthcare IoT as the key purpose of the system is to provide 24-hour monitoring and provide an alarm in case of emergency, which require access to mobile phones [58].

The risk is further amplified due to the fact that healthcare professionals are not experts at cyber security due to the complexity of the technology. Thus, the user interface of cyber security solutions must be easy to understand so the healthcare workforce can play a productive role in safeguarding data breach attempts [60]. The concerns mentioned above are some of the critical broad domains, which are critical areas of cyber-attack and data theft. However, the actual procedures and ways of data theft, such as Eavesdropping, Node Capture, Business Logic Attack, etc, are countless and are outside the scope of this paper [14].

8.2 Ethical Issues

Although the introduction of IoT in healthcare has massive potential to benefit humans in myriad ways, this introduction can also significantly disrupt the lives of humans and work. There is a chance that human contact and closeness will be lost as machines will conduct most of the human business [19]. AI in

particular, will replace the need to meet face-to-face. Human contact is an essential element in healthcare due to the sensitive nature of the field. Thus, this aspect can cause a significant issue in adoption. Similarly, IoT can also replace the work of many humans and cause unemployment leading to wealth inequality and widening the gap between rich and poor [19].

Moreover, novel issues can arise as eventually AI will take off to a situation where humans will no longer have much control [61]. It is without a doubt that mistakes will be made by AI in the diagnosis and treatment at the initial phases and this is also likely that in the case of an incident, the patient may receive medical attention from machines that they actually prefer to receive from empathetic healthcare professionals [61]. Last but not least, the human experts who will create and train AI and IoT can infuse their bias into the system, which can proliferate globally in an unidentified manner. For instance, machine learning systems incorporated in the health sector may be subject to bias in algorithms, perhaps to predict an increased chance of disease detection among certain races or gender, when in reality, these demographics will have no association of any kind with the disease [62].

It has been suggested by many researchers that the greatest challenge of IoT and AI adoption in healthcare is not the efficacy of the technology but the acceptance by the clinicians [61,2]. Considering the above-mentioned factors, it can be concluded that IoT and AI may face substantial issues in adoption and acceptance in the healthcare sector. Despite this, most of the past studies conducted on IoT were focused on either IoT procedural or technical issues. Issues related to knowledge, perception, adoption, motivation, actual use and satisfaction should be well discussed and demand in-depth research. The adoption issues might be related to the above-mentioned aspects, but this is also possible that these would be linked to some other not well-known factors, which also require extensive research.

9. Conclusion

IoT has great potential to transform the world we live in, and it is bringing comfort and convenience into our lives through various interconnected devices and applications. In particular, it can support the healthcare sector by decreasing the load on the hospitals and healthcare clinics, doctors and other medical staff and improving the quality of service. However, IoT adoption in healthcare also faces challenges ranging from data security and privacy.

Acknowledgment

This work is done as a part of a PhD sponsored by the Al Baha University, Kingdom of Saudi Arabia.

References

[1] Yassein, Muneer Bani, Ismail Hmeidi, Marwa Al-Harbi, Lina Mrayan, Wail Mardini, and Yaser Khamayseh. “IoT-Based Healthcare Systems: A Survey.” In Proceedings of the Second International Conference on Data Science, E-Learning and Information Systems - DATA ’19, 1–9, 2019. https://doi.org/10.1145/3368691.3368721.

[2] Al-Rawashdeh, Manal, Pantea Keikhosrokiani, Bahari Belaton, Moatsum Alawida, and Abdalwhab Zwiri. “IoT Adoption and Application for Smart Healthcare: A Systematic Review.” Sensors 22, no. 14 (July 19, 2022): 5377. https://doi.org/10.3390/s22145377.

[3] Madakam, Somayya, R. Ramaswamy, and Siddharth Tripathi. “Internet of Things (IoT): A Literature Review.” Journal of Computer and Communications 03, no. 05 (2015): 164–73. https://doi.org/10.4236/jcc.2015.35021.

[4] Statistics. “Number of Internet and Social Media Users Worldwide as of July 2022. .” Statista. www.statista.com, April 26, 2022. https://www.statista.com/statistics/617136/digital-population-worldwide/.

[5] Diomidous, Marianna, Kostis Chardalias, Adrianna Magita, Panagiotis Koutonias, Paraskevi Panagiotopoulou, and John Mantas. “Social and Psychological Effects of the Internet Use.” Acta Informatica Medica 24, no. 1 (2016): 66. https://doi.org/10.5455/aim.2016.24.66-69.

[6] Naughton, John. “The Evolution of the Internet: From Military Experiment to General Purpose Technology.” Journal of Cyber Policy 1, no. 1 (January 2, 2016): 5–28. https://doi.org/10.1080/23738871.2016.1157619.

[7] Nagajayanthi, B. “Decades of Internet of Things towards Twenty-First Century: A Research-Based Introspective.” Wireless Personal Communications 123 (November 18, 2022): 3661–97. https://doi.org/10.1007/s11277-021-09308-z.

[8] Kramp Thorsten, Rob van Kranenburg, and Sebastian Lange. “Introduction to the Internet of Things.” Enabling Things to Talk, 2013, 1–10. https://doi.org/10.1007/978-3-642-40403-0_1.

[9] Ashton, K. “That ‘Internet of Things’ Thing.” RFID Journal 22, no. 7 (2009): 97–114.

[10] BPB Online. “The Many Names of the Internet of Things (IoT).” DEV Community, 2021. https://dev.to/bpb_online/the-many-names-of-the-internet-of-things-iot-24dc#:~:text=These%20names%20are%20a%20little.

[11] Bayer, Sarah, Henner Gimpel, and Daniel Rau. "IoT-commerce-opportunities for customers through an affordance lens." Electronic Markets 31, no. 1 (2021): 27-50.

[12] Berte, Dan-Radu. “Defining the IoT.” Proceedings of the International Conference on Business Excellence 12, no. 1 (May 1, 2018): 118–28. https://doi.org/10.2478/picbe-2018-0013.

[13] Borycki, Dawid. Programming for the Internet of Things : Using Windows 10 IoT Core and Azure IoT Suite, 2017. https://books.google.com.au/books?id=1_skDwAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

[14] Yıldırım, Muhammed, Uğur Demiroğlu, and Bilal Şenol. “An In-Depth Exam of IoT, IoT Core Components, IoT Layers, and Attack Types.” European Journal of Science and Technology 28 (October 16, 2021): 665–69. https://doi.org/10.31590/ejosat.1010023.

[15] Mouha, Radouan Ait. “Internet of Things (IoT).” Journal of Data Analysis and Information Processing 9, no. 2 (March 18, 2021): 77–101. https://doi.org/10.4236/jdaip.2021.92006.

[16] Khattak Hasan Ali, Munam Ali Shah, Sangeen Khan, Ihsan Ali, and Muhammad Imran. “Perception Layer Security in Internet of Things.” Future Generation Computer Systems 100 (November 2019): 144–64. https://doi.org/10.1016/j.future.2019.04.038.

[17] Nižetić, Sandro, Petar Šolić, Diego López-de-Ipiña González-de-Artaza, and Luigi Patrono. “Internet of Things (IoT): Opportunities, Issues and Challenges towards a Smart and Sustainable Future.” Journal of Cleaner Production 274 (November 2020): 122877. https://doi.org/10.1016/j.jclepro.2020.122877.

[18] Ghosh, Ashish, Debasrita Chakraborty, and Anwesha Law. “Artificial Intelligence in Internet of Things.” CAAI Transactions on Intelligence Technology 3, no. 4 (December 1, 2018): 208–18. https://doi.org/10.1049/trit.2018.1008.

[19] Tai, Michael Cheng-Tek. “The Impact of Artificial Intelligence on Human Society and Bioethics.” Tzu Chi Medical Journal 32, no. 4 (August 14, 2020): 339. https://doi.org/10.4103/tcmj.tcmj_71_20.

[20] Kumar, Sachin, Prayag Tiwari, and Mikhail Zymbler. “Internet of Things Is a Revolutionary Approach for Future Technology Enhancement: A Review.” Journal of Big Data 6, no. 1 (December 2019). https://doi.org/10.1186/s40537-019-0268-2.

[21] Zanella, Andrea, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi. “Internet of Things for Smart Cities.” IEEE Internet of Things Journal 1, no. 1 (February 2014): 22–32. https://doi.org/10.1109/jiot.2014.2306328.

[22] Khajenasiri, Iman, Abouzar Estebsari, Marian Verhelst, and Georges Gielen. “A Review on Internet of Things Solutions for Intelligent Energy Control in Buildings for Smart City Applications.” Energy Procedia 111 (March 1, 2017): 770–79. https://doi.org/10.1016/j.egypro.2017.03.239.

[23] NEOM. “The Line New Wonders of the World.” www.neom.com, 2022. https://www.neom.com/en-us/regions/theline.

[24] Fraga, Kaleena. “Construction Begins on ‘the Line,’ a 105-Mile-Long Megacity in Saudi Arabia That’s Right out of a Sci-Fi Movie.” All That’s Interesting, 2022. https://allthatsinteresting.com/saudi-arabia-the-line.

[25] Onasanya, Adeniyi, and Maher Elshakankiri. “Smart Integrated IoT Healthcare System for Cancer Care.” Wireless Networks 27, no. 6 (January 2, 2021): 4297–4312. https://doi.org/10.1007/s11276-018-01932-1.

[26] Singh, Ravi Pratap, Mohd Javaid, Abid Haleem, and Rajiv Suman. “Internet of Things (IoT) Applications to Fight against COVID-19 Pandemic.” Diabetes & Metabolic Syndrome: Clinical Research & Reviews 14, no. 4 (May 2020): 521–24. https://doi.org/10.1016/j.dsx.2020.04.041.

[27] Tyagi, Sapna, Amit Agarwal, and Piyush Maheshwari. “A Conceptual Framework for IoT-Based Healthcare System Using Cloud Computing.” IEEE Xplore, January 1, 2016, 503–7. https://doi.org/10.1109/CONFLUENCE.2016.7508172.

[28] Kim, Suwon, and Seongcheol Kim. “User Preference for an IoT Healthcare Application for Lifestyle Disease Management.” Telecommunications Policy 42, no. 4 (May 2018): 304–14. https://doi.org/10.1016/j.telpol.2017.03.006.

[29] Ahmadi, Hossein, Goli Arji, Leila Shahmoradi, Reza Safdari, Mehrbakhsh Nilashi, and Mojtaba Alizadeh. “The Application of Internet of Things in Healthcare: A Systematic Literature Review and Classification.” Universal Access in the Information Society 18 (May 4, 2018): 837–69. https://doi.org/10.1007/s10209-018-0618-4.

[30] Marengoni, Alessandra, Sara Angleman, René Melis, Francesca Mangialasche, Anita Karp, Annika Garmen, Bettina Meinow, and Laura Fratiglioni. “Aging with Multimorbidity: A Systematic Review of the Literature.” Ageing Research Reviews 10, no. 4 (September 2011): 430–39. https://doi.org/10.1016/j.arr.2011.03.003.

[31] Branger, Jakob, and Zhibo Pang. “From Automated Home to Sustainable, Healthy and Manufacturing Home: A New Story Enabled by the Internet-of-Things and Industry 4.0.” Journal of Management Analytics 2, no. 4 (October 2, 2015): 314–32. https://doi.org/10.1080/23270012.2015.1115379.

[32] Ludwig, Wolfram, Klaus-Hendrik Wolf, Christopher Duwenkamp, Nathalie Gusew, Nils Hellrung, Michael Marschollek, Markus Wagner, and Reinhold Haux. “Health-Enabling Technologies for the Elderly – an Overview of

Services Based on a Literature Review." Computer Methods and Programs in Biomedicine 106, no. 2 (May 2012): 70–78. https://doi.org/10.1016/j.cmpb.2011.11.001.

[33] Granados, Jose, Tomi Westerlund, Lirong Zheng, and Zhuo Zou. "IoT platform for real-time multichannel ECG monitoring and classification with neural networks." In Research and Practical Issues of Enterprise Information Systems: 11th IFIP WG 8.9 Working Conference, CONFENIS 2017, Shanghai, China, October 18-20, 2017, Revised Selected Papers 11, pp. 181-191. Springer International Publishing, 2018.

[34] Tekeste, Temesghen, Hani Saleh, Baker Mohammad, and Mohammed Ismail. "Ultra-Low Power QRS Detection and ECG Compression Architecture for IoT Healthcare Devices." IEEE Transactions on Circuits and Systems I: Regular Papers 66, no. 2 (September 27, 2018): 669–79. https://doi.org/10.1109/tcsi.2018.2867746.

[35] Satija, Udit, Barathram Ramkumar, and M S Manikandan. "Real-Time Signal Quality-Aware ECG Telemetry System for IoT-Based Health Care Monitoring." IEEE Internet of Things Journal 4, no. 3 (June 2017): 815–23. https://doi.org/10.1109/jiot.2017.2670022.

[36] Saikumar, K., V. Rajesh, Gautam Srivastava, and Jerry Chun-Wei Lin. "Heart Disease Detection Based on Internet of Things Data Using Linear Quadratic Discriminant Analysis and a Deep Graph Convolutional Neural Network." Frontiers in Computational Neuroscience 16 (October 7, 2022). https://doi.org/10.3389/fncom.2022.964686.

[37] Mulac, Alma, Katja Taxis, Ellen Hagesaether, and Anne Gerd Granas. "Severe and Fatal Medication Errors in Hospitals: Findings from the Norwegian Incident Reporting System." European Journal of Hospital Pharmacy28, no. 1 (June 23, 2021). https://doi.org/10.1136/ejhpharm-2020-002298.

[38] John Hopkins Medicine. "Study Suggests Medical Errors Now Third Leading Cause of Death in the U.S. - 05/03/2016." Hopkinsmedicine.org, 2016. https://www.hopkinsmedicine.org/news/media/releases/study_suggests_medical_errors_now_third_leading_cause_of_death_in_the_us.

[39] Shrivastava, Akash. "Exploring the Smartwatch as a Tool for Medical Adherence." Master's thesis, 2015. https://www.diva-portal.org/smash/get/diva2:824289/FULLTEXT01.pdf.

[40] Baqir, Wasim, Kate Jones, William Horsley, Scott Barrett, David Fisher, Richard Copeland, David Campbell, and Rosemary Stephenson. "Reducing Unacceptable Missed Doses: Pharmacy Assistant-Supported Medicine Administration." International Journal of Pharmacy Practice 23, no. 5 (January 28, 2015): 327–32. https://doi.org/10.1111/ijpp.12172.

[41] Serdaroglu, Kemal, Gamze Uslu, and Sebnem Baydere. "Medication Intake Adherence with Real Time Activity Recognition on IoT." In IEEE Xplore, 230–37, 2015. https://doi.org/10.1109/WiMOB.2015.7347966.

[42] Dillner, Joakim. "Early Detection and Prevention." Molecular Oncology 13, no. 3 (March 1, 2019): 591–98. https://doi.org/10.1002/1878-0261.12459.

[43] Jagadeeswari, V., V. Subramaniyaswamy, R. Logesh, and V. Vijayakumar. "A Study on Medical Internet of Things and Big Data in Personalized Healthcare System." Health Information Science and Systems 6, no. 1 (September 20, 2018). https://doi.org/10.1007/s13755-018-0049-x.

[44] Sareen, Sanjay, Sandeep K. Sood, and Sunil Kumar Gupta. "Secure Internet Of Things-Based Cloud Framework To Control Zika Virus Outbreak." International Journal of Technology Assessment in Health Care 33, no. 1 (2017): 11–18. https://doi.org/10.1017/s0266462317000113.

[45] Nasajpour, Mohammad, Seyedamin Pouriyeh, Reza M. Parizi, Mohsen Dorodchi, Maria Valero, and Hamid R. Arabnia. "Internet of Things for Current COVID-19 and Future Pandemics: An Exploratory Study." Journal of Healthcare Informatics Research 4, no. 4 (November 12, 2020): 325–64. https://doi.org/10.1007/s41666-020-00080-6.

[46] Kollu, Praveen Kumar, Kailash Kumar, Pravin R. Kshirsagar, Saiful Islam, Quadri Noorulhasan Naveed, Mohammad Rashid Hussain, and Venkatesa Prabhu Sundramurthy. "Development of Advanced Artificial Intelligence and IoT Automation in the Crisis of COVID-19 Detection." Journal of Healthcare Engineering 2022 (March 2, 2022): e1987917. https://doi.org/10.1155/2022/1987917.

[47] CDC. "Coronavirus Disease 2019 (COVID-19) – Symptoms." Mayo Clinic, March 22, 2020. https://www.CDC.gov/coronavirus/2019-ncov/symptoms-testing/symptoms.html.

[48] Handley, Rich. "How IoT Sensors Can Help Detect and Control Contagious Diseases." RFID JOURNAL, June 21, 2020. https://www.rfidjournal.com/how-iot-sensors-can-help-detect-and-control-contagious-diseases.

[49] Mohammed, M, Nurul Hazairin, S Al-Zubaidi, Safinaz Mustapha, and Eddy Yusuf. "TOWARD a NOVEL DESIGN for CORONAVIRUS DETECTION and DIAGNOSIS SYSTEM USING IOT BASED DRONE TECHNOLOGY." International Journal of Psychosocial Rehabilitation 24, no. 7 (2020a): 2020.

[50] Mohammed , M, Halim Syamsudin, S Al-Zubaidi, Rusyaizila Ramli, and Eddy Yusuf. "NOVEL COVID-19 DETECTION and DIAGNOSIS SYSTEM USING IOT BASED SMART HELMET." International Journal of Psychosocial Rehabilitation 24, no. 7 (2020b): 2020.

[51] Ruktanonchai, Nick Warren, Corrine Warren Ruktanonchai, Jessica Rhona Floyd, and Andrew J. Tatem. "Using Google Location History Data to Quantify Fine-Scale Human Mobility." International Journal of Health Geographics 17, no. 28 (July 27, 2018): 1–13. https://doi.org/10.1186/s12942-018-0150-z.

[52] Ghosh, Shona. "Police in China, Dubai, and Italy Are Using These Surveillance Helmets to Scan People for COVID-19 Fever as They Walk Past and It May Be Our Future Normal." Business Insider, 2020. https://www.businessinsider.com/coronavirus-italy-holland-china-temperature-scanning-helmets-2020-5.

[53] Haleem, Abid, Mohd Javaid, Raju Vaishya, and S.G. Deshmukh. "Areas of Academic Research with the Impact of COVID-19." The American Journal of Emergency Medicine 38, no. 7 (April 2020): 1524–26. https://doi.org/10.1016/j.ajem.2020.04.022.

[54] Chamola, Vinay, Vikas Hassija, Vatsal Gupta, and Mohsen Guizani. "A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain and 5G in Managing Its Impact." IEEE Access 8 (2020): 1–1. https://doi.org/10.1109/access.2020.2992341.

[55] Pennic, Fred. "'Pandemic Drone' Could Detect Virus Symptoms like COVID-19 in Crowds." hitconsultant.net, 2020. https://hitconsultant.net/2020/03/27/pandemic-drone-could-detect-virus-symptoms-like-covid-19-in-crowds/.

[56] Gatsis, K, and G J Pappas. "Poster Abstract: Wireless Control for the IoT: Power, Spectrum, and Security Challenges." In 2017 IEEE/ACM Second International Conference on InternetofThings Design and Implementation (IoTDI), 341–42, 2017.

[57] Babovic, Zoran B., Jelica Protic, and Veljko Milutinovic. "Web Performance Evaluation for Internet of Things Applications." IEEE Access 4 (2016): 6974–92. https://doi.org/10.1109/access.2016.2615181.

[58] Perwej , Y, Nikhat Akhtar, Neha Kulshrestha, and Pavan Mishra. "A Methodical Analysis of Medical Internet of Things (MIoT) Security and Privacy in Current and Future Trends." Journal of Emerging Technologies and Innovative Research 9 (January 22, 2022): 346–71. https://doi.org/10.6084/m9.figshare.JETIR2201346.

[59] IBM. "Cost of a Data Breach Report 2020 2 Contents," 2020. https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf.

[60] Xu, Yanchen, Daniel Tran, Yuan Tian, and Homa Alemzadeh. "Analysis of Cyber-Security Vulnerabilities of Interconnected Medical Devices." In IEEE Xplore, 23–24, 2019. https://doi.org/10.1109/CHASE48038.2019.00017.

[61] Davenport, Thomas, and Ravi Kalakota. "The Potential for Artificial Intelligence in Healthcare." Future Healthcare Journal 6, no. 2 (June 2019): 94–98. https://doi.org/10.7861/futurehosp.6-2-94.

[62] Davenport, Thomas H, and Keith J Dreyer. "AI Will Change Radiology, but It Won't Replace Radiologists." Harvard Business Review, 2018. https://hbr.org/2018/03/ai-will-change-radiology-but-it-wont-replace-radiologists.

Abdulaziz Alomari: He received the B.E. and M.E. degrees, from Al Baha Univ and La Trobe Univ in 2007 and 2018, respectively. He is currently a PhD candidate in Computer Science at La Trobe Univ. He has been a lecturer at Al Baha Univ since 2012. His research interests include IoT, Cloud Computing and AI.

Ben Soh: Associate Professor Ben Soh obtained his PhD in Computer Science & Engineering (in the area of Secure and Fault-Tolerant Computing under the tutelage of Prof TS Dillon) from La Trobe. Since then, he has successfully supervised to completion 13 PhD students and published more than 200 peer-reviewed research papers. He has made significant contributions in the following research areas: Fault-Tolerant and Secure Computing, Cloud Computing, Information Systems Research, Pervasive Wireless Network Communications, Educational Technology and Business Process Management. Currently he is La Trobe Cybersecurity Programs Advisor/Coordinator.