Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Industrial internet of things: Investigation of the applications, issues, and challenges

Shakir Khan *, Mohammed Altayar

College of Computer and Information Sciences, Imam Mohammad ibn Saud Islamic University, Riyadh, Saudi Arabia

ARTICLE INFO

Article history:
Received 31 March 2020
Received in revised form
16 August 2020
Accepted 4 September 2020

Keywords:
Industrial internet of things
Recent technologies
IoT applications
IoT challenges
Industrial cities network
Industrial surroundings
Industrial agriculture

ABSTRACT

The Internet of Things (IoT) is increasingly becoming a major component of contemporary societies and the next stage of the Internet's development. Its applications have touched several aspects of our lives, including health, economy, technology, education, environment, and transport. In addition, recent research shows that interest in the IoT is increasing, driven by the potential benefits that it brings, such as improving efficiency and productivity, saving time and effort, staying connected, better health services and care, improved safety and security, automation and control among other benefits. However, despite these advantages and due to the infancy of the IoT, research around this topic is still evolving, and more needs to be done to understand this paradigm of technology. This paper aims to review current applications and challenges associated with its adoption. It provides insights into current applications of the IoT in different domains, including smart cities, health care, smart agriculture, smart water management, retail, logistic and product lifetime management, smart living, public safety and environmental monitoring, and the IoT for physically challenged persons. Concerning the challenges, the study discusses issues related to confidentiality, security, and privacy, data management, machine-to-machine communication, interoperability, reliability, availability and robustness, technological architecture issues, and standardization. Finally, the study concludes with a summary of the findings and suggestions for future research.

1. Introduction

The Internet is defined as a network of connected computers that communicate by linking entities and producing information. The Internet of Things (IoT) is the next generation of the Internet that integrates different ranges of technologies such as sensory, communication, networking, and intelligent technologies for the purpose of handling and processing information (Li et al., 2016). The power of the IoT does not only consist of remote control. Another important benefit of connecting objects is the possibility for smart objects to access any kind of information through the Internet, information that can be exploited to improve the service offered to end-users (Husein, 2019; Righetti et al., 2018). The networking giant's latest mobile Visual Networking Index (VNI) forecast estimates that there will be more than 12 billion connected mobile devices across the world by 2022, up from nine billion today (Dhanda et al., 2019).

The Internet is continuously developing as expected, but recently it has developed additional than merely a connected grid of workstations, but a network of many devices (Husein, 2019). The IoT functions as a network of different 'connected' devices, or a network of networks (Miraz et al., 2018), as revealed in Fig. 1. Currently, appliances such as smartphones, vehicles, industrial systems, healthcare appliances, cameras, toys, buildings, home appliances, industrial systems, and countless others can all make up part of the information shared in excess of the Internet. Irrespective of their dimensions and utilities, these policies can perform industrial reformations, tracking, locating, controlling, real-time monitoring, and process controlling. There has been a significant increase in Internet-enabled devices. Even however its furthermost important commercial result has been in the personal microchip technology field, seen in the rebellion of smartphones and wearable devices,

* Corresponding Author.
Email Address: sgkhan@imamu.edu.sa (S. Khan)
https://doi.org/10.21833/ijaas.2021.01.013
Corresponding author's ORCID profile:
https://orcid.org/0000-0002-7925-9191

such as watches and headsets, joining persons has become simply one part of a higher movement towards the fusion of the digital and physical worlds (Husein, 2019). The IoT is projected to continue expanding its influence, which will affect the appliances and utilities that it can track. This is obvious from the uncertainty in the appearance of 'things,' which makes it challenging to plan the increasing limits of the IoT (Husein, 2019). The IoT marks the first real evolution of the Internet. This paper aims to review current applications and challenges associated with IoT adoption. Section 2 discusses elements of the IoT's potential applications. This is followed by Section 3, which discusses various IoT challenges and issues. Finally, a conclusion is drawn in Section 4.

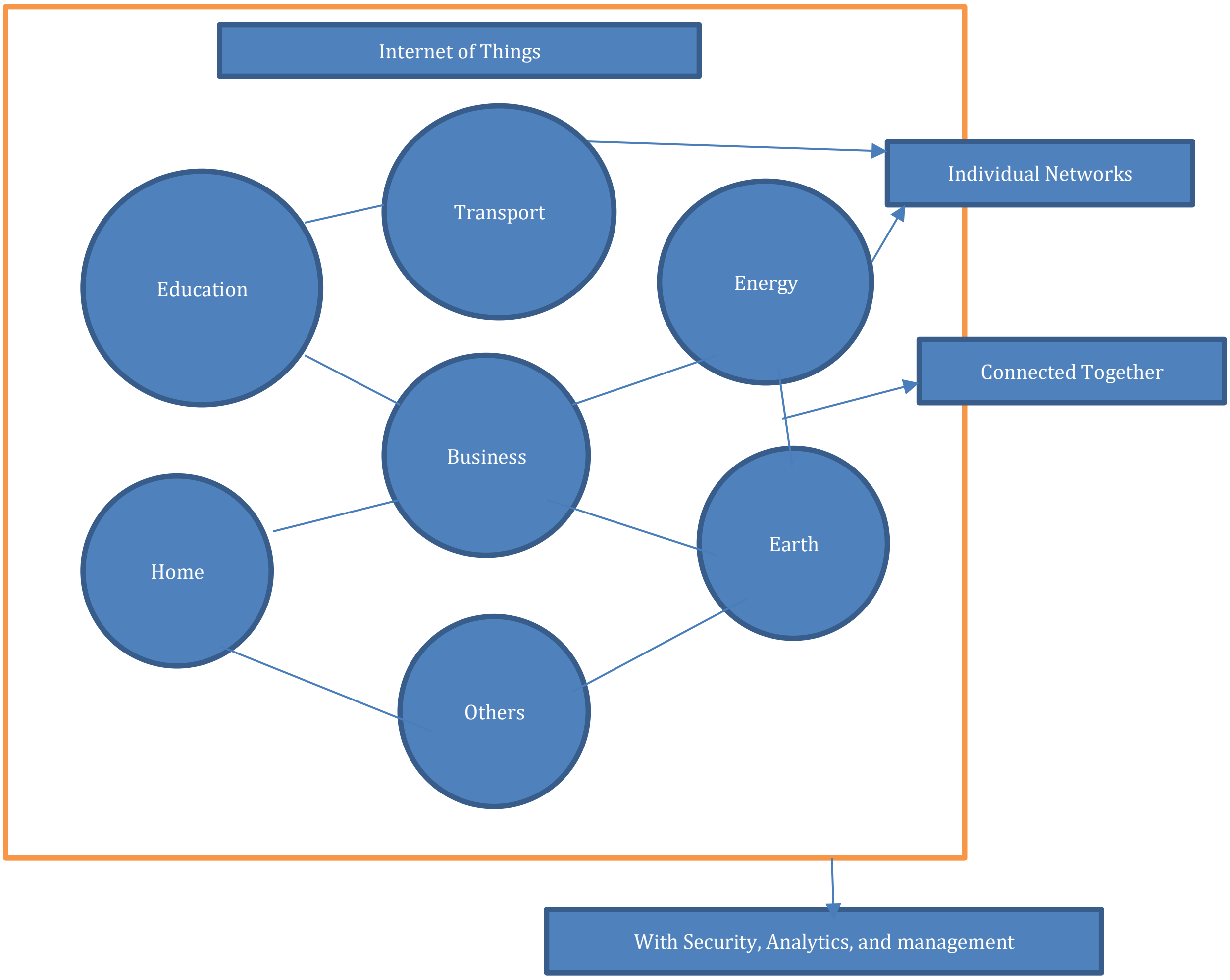

Fig. 1: IoT as a network of network (Husein, 2019)

2. Prospective application domains of IoT

The number of IoT applications is progressively growing and promises to bring immense value to our lives. With newer wireless networks, superior sensors, and revolutionary computing capabilities, the IoT could be the next frontier in the race for a share of the wallet. The following is a discussion of the potential applications of the IoT that can be applied in many areas.

2.1. Smart cities and urbanization

The number of IoT applications for smart cities is gradually increasing. Progressively more cities are installing sensors and actuators to hypothetically implement all the actions that are voted for in the city. Such strategies classically connect using end to end wireless connections and generate a kind of passageway system saturating the city. Eco-friendly observing, traffic monitoring, smart parking, smart following, and hands-on sensing are some of the unbiased collection applications previously applied in many cities. A brief summary of these applications is provided below, emphasizing their benefits for the populace but also highlighting their possible fears. Due to space limitations, a limited number of applications are mentioned (Kumar et al., 2019). According to Sodhro et al. (2018), IoT provides an essential aspect of the elegance of cities and improving their overall structure. Some aspects of the utilization of the IoT in constructing industrial cities consist of industrial construction, traffic jamming (Woznowski et al., 2016; Soomro et al., 2018), waste management (Mahmud et al., 2018), industrial transportation systems (Woznowski et al., 2016), industrial lighting, industrial car parks, and town maps. These may comprise seemingly different functionalities, for instance, observing existing car park spaces inside the town, observing phenomena and the measurable conditions of links and buildings, placing rigorous checking devices in houses in sensitive parts of cities, and detecting numbers of walkers and means of transportation. An artificial intelligence (AI) collective using the IoT has the ability to report on important challenges modeled by some city groups, which consist of traffic organization, healthcare, energy disasters, and several other issues. This can improve the lives of the residents and businesses in a smart city. Before diving into the joining part, let us discover some of the mechanisms of smart cities. A smart town has countless use cases for AI-driven IoT supported technology, from conserving an improved environment to enhancing community transportation and security. The application of the IoT to accomplish smart cities would require systematic radio-frequency identification. According to Husein (2019), being equipped with interrelated devices and actuators is a component of a machine that is responsible for moving and controlling a mechanism or system to observe any activity inside a building. Most actions will be computerized based on data collected by sensors and/or inclinations communicated by the user or concluded by the classification itself.

2.2. Medical care

The IoT healthcare network or the IoT network for health care (hereafter 'the IoThNet') is one of the main components of the IoT in health care. It supports access to the IoT's strengths, facilitates the communication and treatment of medical data, and enables the use of healthcare-tailored communications. As shown in Fig. 2, this section discusses the IoThNet topology, architecture, and platform (Zhu et al., 2010). It should be seen that the planned architectures in Grønbæk (2008) and Dagar et al. (2018) can be well-thought-out as a good starting point for a growing understanding of the IoT network. Healthcare organizations in several countries are not capable, in their resources and training, and can make mistakes. This can efficiently be transformed with the application of smart strategies that can be computerized and upgraded through equipment. Further, equipment that simplifies processes effortlessly, such as reporting on the distribution of people and area, record protection, and distributing medicines, would go a long way in altering the medical field.

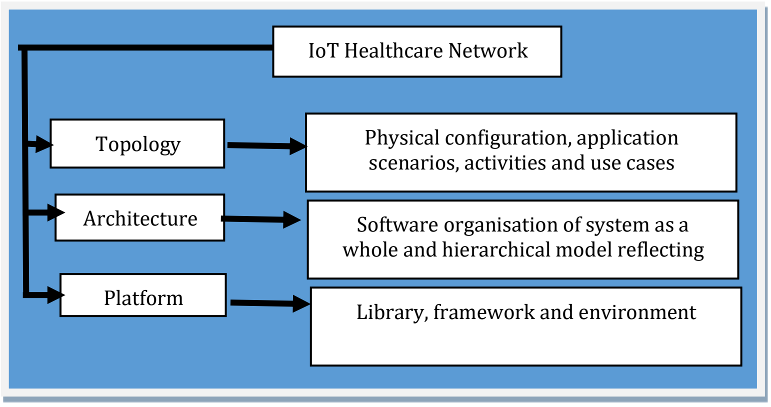

Fig. 2: IoT healthcare network (IoThNet) (Čolaković and Hadžialić, 2018)

IoT devices tagged with sensors are utilized for tracking the real-time position of the medical apparatus, such as wheelchairs, nebulizers, defibrillators, oxygen pumps, and other observing equipment. The placement of medical staff at diverse locations can also be examined in real-time (Sodhro et al., 2018). The use of the IoT in healthcare allows for the automation of processes that have previously taken time; these processes previously allowed human error. For example, nowadays, many hospitals use connected devices to control the airflow and temperature in operating theatres. The advantages of IoT in healthcare are seemingly endless, but these are just a few of the major benefits. The improvements in the IoT and the Internet of Everything are, moreover, being drawn out slowly, as shown by the emergence of the Internet of Nano-Things (IoNT) (Husein, 2019; Miraz et al., 2018). As the label suggests about the concept of the IoNT, is actuality planned by incorporating nano-sensors in different substances (things) to make up nanonetworks. Healing deployment, as displayed in Fig. 3, is one of the first motivations for the development of the IoNT.

2.3. Agriculture sector

Smart agriculture is the application of several types of machinery and devices such as the Internet, cloud, and IoT devices (Kamienski et al., 2018a). As the population of the world is growing and it is expected to be around 9.7 billion by 2050, to nourish those billions of people, we must advance the production of food. On the other hand, the farmed land is being reduced because of various issues, including mechanization, commercial markets, and housing construction taking place on farmland. However, to feed those billions, we require an increase in agriculture, and this can be accomplished by using the IoT. Smart agriculture is also known as precision agriculture. The current farming situation is not appreciated by agriculturalists for many reasons, including pest attacks, plant sickness, lack of knowledge of vital supplements for the yields, and numerous other difficulties. In order to remove these difficulties and make agriculture more profitable, smart, and approachable for agriculturalists, they need high-tech advancement.

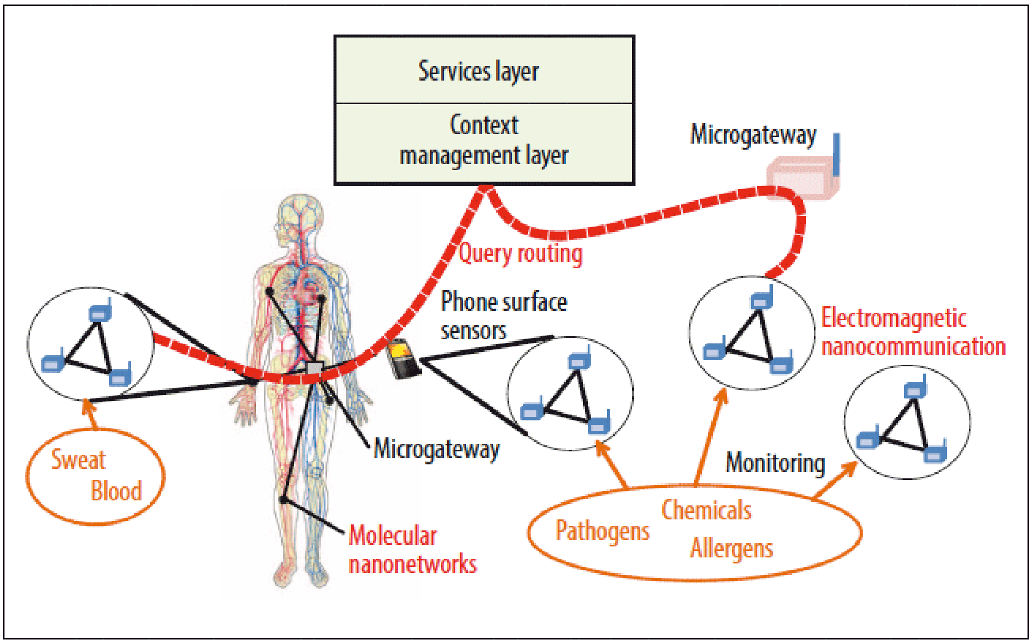

Fig. 3: The internet of nano-things (Husein, 2019)

Old-style agriculture and precision agriculture are different from each other in every way. Old-style agriculture practices the old and outdated methods of cultivation, employing those ancient devices for work and planting regular crops without any evaluation of difficulties in the market, rates, or climate reports. Smart farming uses innovative technologies, including smart connected devices, IoT devices, the Internet, communication, and the periodical evaluation of many factors, such as the best circumstances for vegetables to grow, what nutrients are required, soil excellence, and water superiority checks. Smart agriculture makes agriculture easy and inexpensive (cost-effective), reduces labor costs, increases harvest yields, and delivers healthier production. As discussed by Husein (2019) and Veena et al. (2018), the IoT has the capability of supporting the improvement of the agricultural sector by investigating soil humidity levels and, in the case of wineries, observing the stem diameters. The IoT would enable agriculturists to maintain and control the number of vitamins set up in farming yields and to control microclimate circumstances in order to create the best growth and excellence of root vegetables and fruits. Additionally, considering the current climate circumstances, the IoT would allow for the prediction of incoming rain or snow, deficiencies, and wind variations, thus allowing for temperature and moisture levels to be adjusted to stop fungus and other microbial pollutants.

2.4. Smart water management

A water shortage is the absence of adequate existing water resources to meet the requirements of water usage inside a province, which is, according to the United Nations Development Programme, produced mostly by unsuccessful management of resources, disturbing around 1.2 billion individuals in various parts of the world. The IoT, as a system, comprehends countless possibilities to resolve severe problems in numerous aspects of our everyday life, including water shortages, via smart, instantaneous, and expected management. In each part of the water cycle, the IoT can be useful to make water resources healthier and achieve well-organized and optimal outcomes.

As clarified by Husein (2019), Veena et al. (2018), Kamienski et al. (2018b), and Kor et al. (2016), moreover, a town can be smart when they have homes that are also smart in terms of waste controlling, energy preserving, water preserving, and environment preserving. IoT equipment also has advantages in developing the maintenance and control of pumps on a systematic basis for correctly controlling the use of water. The SWAMP project progresses IoT-based methods and tactics for smart water control in the precision irrigation domain and guides them in Italy, Spain, and Brazil. IoT and other technologies are the accepted choice for smart water control applications, and the SWAMP project is predicted to verify the suitability of IoT in actual surroundings with the arrangement of on-site pilots.

2.5. Supply chain, retail, and products management

An original significant illustration of an industrialized IoT submission is managing the strategy and inventory series. RFIDs can be allocated towards substances besides recycled to recognize supplies and belongings, including clothes, fixtures, apparatus, foodstuff, and water (Villanueva et al., 2012; Borgia, 2014). Their usage supports efficiency in warehouses and trades and streamlining records by giving precise facts of the present record while decreasing record mistakes. The whole lifecycle of substances can be followed (Cai et al., 2014; Borgia, 2014). For instance, RFID readers connected in the manufacturing plant enable the screening of the manufacturing procedure, and the tag can be marked out all over the whole inventory sequence (e.g., wrapping, shipping, loading, sale to the consumer, throwing away). Forward-thinking IoT systems, self-possessed of RFID-furnished substances and shrewd devices tracing substances in actual, may help by substantially decreasing unwanted, thus reducing costs and enlightening turnover restrictions for both merchants and producers. According to Borgia (2014), an estimated 8.3% drop in sales has been predicted if drops keep on partly allowed of goods. Inadequate production and excessive production may decrease radically by using an accurate evaluation of desired substances, which can be conditional by investigating data composed by shrewd tags (Gruen et al., 2002). Additionally, the real-time investigation by sensors permits the classification of product decline procedures for foodstuff and water with dynamic significance. Such as confirming the bloom of decayable (e.g., fruits, root vegetables, icy food), devices may endlessly screen heat plus moisture privileged storage containers or freezers, and controllers may adjust these, creating ideal management of the enclosed food. In addition, product reliability may be improved with RFID founded validation developments. Supplementary fascinating IoT bids are smart supermarket run coordination. Such systems observe operators' buying behaviors by tracing their portable phones and direct them in factories/superstores/malls to reduced items or service in loose expense processes (e.g., spontaneous check-out exhausting bionomics) (Borgia, 2014). Using the IoT also supports repairs and renovations because engineers can be sent to homes that forecast tool failures and, at the same time, periodic repairs can be automatically scheduled before there is an equipment malfunction. This can be attained through the installing of tags in classified equipment or technology to screen performance and occasionally guide information (Borgia, 2014; Tadejko, 2015).

2.6. Smart living

A smart living will incorporate the following: smart home computerization, protection, and security. Smart sensors can be employed to bring together important data about the home. For instance, smart sensors could save data about tenants and landowners' temperature choices, followed by applicable variations. Samsung has launched the Smart Home Ecosystem, which connects home devices (e.g., TV set, home appliances, and smartphones) by means of a single incorporated platform. These devices can be organized by users with an application that connects the devices in a household. Samsung SmartThings Starter Kit offers the whole setup required to make a smart home. It is iOS, Android, and Windows Mobile friendly. The SmartThings Starter Kit offers the following functionalities: (i) home observation from everywhere; (ii) home control with an app; (iii) home safety and security from loss and threat; and (iv) scalability by developing hundreds of well-matched smart devices to boost home computerization. Its components include a pivot to attach smart sensors, decorations, locks, cameras, a gesture sensor to observe effort in the home, a multi-sensor to observe whether doors, frames, drawers, or garages are exposed or locked, an occurrence sensor to recognize when individuals, animals, and cars come to or leave home and a power channel to rheostat lights, electronics, and small appliances. The Smart Home Cloud API (Dastbaz et al., 2017) offers approaches to switch and display Samsung Smart Home operations. Through this Smart Home Control Service, a partner's product can unite with numerous devices and provide better services to their purchaser. This service functions from end to end with cloud-to-cloud incorporation between the partner cloud and the Smart Home cloud. This is enabled by the running of numerous REST APIs by Samsung for associates, so they are able to coordinate with the Samsung Smart Home cloud. The body of the REST API utilizes a standard JSON certificate (called Smart Home Data), which means that associate developers are required to know the JSON document (Dastbaz et al., 2017). Besides this, smart homes are expected to evolve significantly and will be able to anticipate and meet the needs of their owners or occupants, even without being asked. For example, the AI devices will be able to know what music a person wants to hear at a certain time of the day and play it for them and will check their daily task schedule and reset the alarm daily according to this schedule. When the person wakes up, the bathtub will be prepared and filled with water that matches the person's body temperature. Also, Smart Home applications as one of the elements of smart cities are individually the most demanded application without question. Moreover, washing machines can permit one to monitor laundry distantly. Additionally, an extensive range of kitchen appliances can be reached via a smartphone, hence making it conceivable to regulate temperature, as in the case of a microwave. Microwaves that have a self-cleaning component can be checked easily as well. In terms of household security, the IoT can be useful for alarm arrangements, and cameras can be mounted to display and discover when windows or doors are opened, thereby stopping trespassers (Husein, 2019; Miraz et al., 2018).

2.7. Public safety and environmental monitoring

The objective of Native and nation-wide governments is to form a protected culture by ensuring community security and by designing crisis control precisely. The community sanctuary facilities comprise the preservation of community order, the avoidance and defense of nations, and the protection of the community and private belongings. Disaster organization supports the people in planning for and handling natural or artificial tragedies, such as biological leaks, torrents, storms, earthquakes, cyclones, floods, and the loss of the electrical power network supply to an end-user. The IoT compromises elucidations for observing plus undertaking such disaster situations (Borgia, 2014). Statistics combined from security cameras placed inside the town and on individual legal resident's strategies permit continuous cinematic observation and defensive observation facilities even though serving the forces as a mechanism for community direction in the circumstance of sporting occasions, harmonious shows, and politically aware gatherings. The security of isolated, in addition, community constructions (e.g., malls, workshops) can be protected with the use of device technology that will activate during disturbances. Crisis processes can be value-added and reinforced by custom IoT technologies. Presently, the emergency system is deficient in exact facts about disaster sites. Devoted devices and smart camcorder along with GPS and to communicate without using cables and wireless technologies providing real-time localization and tracking can be used to form a complete map of the event to forecast its trends (e.g., direction and/or speed of fire spread, major risk areas), and thus to establish a dynamic emergency plan to coordinate the rescue operations. Let's take an example of an intensity in an office block somewhere the entry is prearranged over and done with e-cards. If individuals have to put-down their individual access cards to cross the threshold of the building, the ladder man will identify the precise digit of persons in the construction and anywhere they are located (if the structure has a localization scheme) and are intelligent to escort people in the direction of the closest escape road or to escort firefighters to except stuck people. Furthermore, records from wireless cinematic cameras and other equipment installed on the firefighters' helmets will deliver real-time statistics on the fire development to estimate the finest seepage routes and/or construction downfall time. Agitations are caused by habiliment sensors on firefighters (Borgia, 2014).

2.8. IoT for physically challenged persons

IoT can be fantastically helpful for resolving the difficulties of physically or specially challenged people in their everyday life. Innovative IoT-built Internet or network managed applications can be planned while observing the strategies of the Department of Empowerment of Persons with Disabilities (DEPwD) [Ministry of Social Justice and Empowerment], which has an ongoing Reachable India Campaign (Sugamya Bharat Abhiyan), a cross-country movement to recognize universal suitability for Physically Challenged and Persons with Disabilities (PwDs) (Chaudhary et al., 2019). Fig. 4 shows Figurative Depiction of Applications of IoT for Physically Challenged Persons.

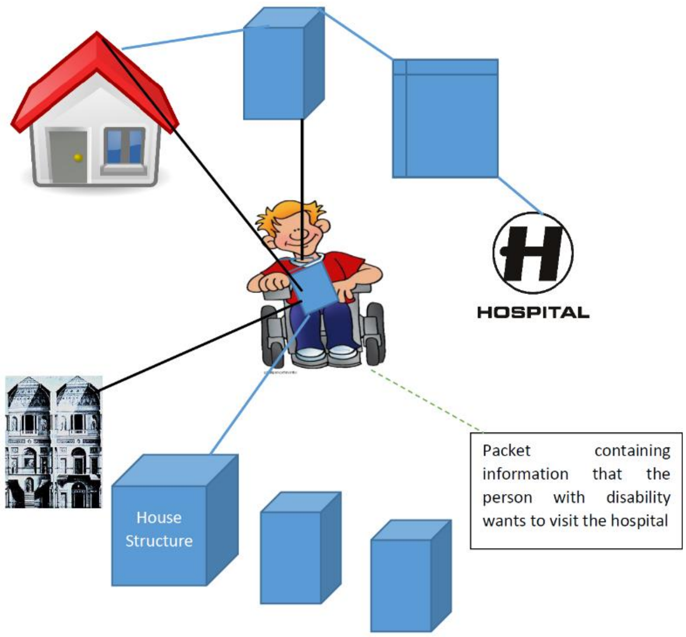

Fig. 4: Figurative depiction of applications of IoT for physically challenged persons (Chaudhary et al., 2019)

3. IoT challenges

The use and adoption of the IoT are likely to result in a number of challenging issues that need consideration. This is due to a number of factors, including the mushrooming number and type of devices and sensors, the vast amount of sensitive data generated by people and smart objects, and the growing number of emerging products and services affecting people's daily lives (Dixit et al., 2015). Researchers have addressed various challenges and problems associated with the IoT. The following is a discussion of these issues.

3.1. Confidentiality, security, and privacy issues

Security gaps that occur in traditional IT systems are likely to be present in the IoT environment but not addressed very well. Since IoT devices generate, collect and distribute a huge amount of data, and part of this data is about users and their behaviors, interactions, and habits, it is not surprising to find that security and privacy are some of the most important issues that need consideration (Dixit et al., 2015; Padyab and Ståhlbröst, 2018; Xu et al., 2018; Husein, 2019). The adoption of new business models and applications that are based on the IoT requires robust security and privacy measures (Chaudhary et al., 2019). This is because the IoT is based on the existing wireless sensor networks (WSN); therefore, it inherits the common security and privacy issues associated with WSN (Husein, 2019). According to Weber (2010), four broad areas related to security and privacy requirements must be addressed, including resistance to attacks, data authentication, and access control, and client privacy. Similarly, other researchers have reported a number of security and privacy issues, including identification, confidentiality, integrity, non-repudiation authentication and authorization, cryptographic security services, trustworthiness, and the message integrity (Vermesan and Friess, 2013; Chaudhary et al., 2019; Husein, 2019). Furthermore, some researchers have addressed security and privacy issues from a legal perspective and suggested that data collection, sharing, and distribution via IoT sensors, applications, and networks must be conducted within existing policies, laws, and regulations, as there is a lack of laws at national and international levels that govern IoT practices (Weber, 2010; Ahlmeyer and Chircu, 2016; Ma et al., 2018).

3.2. Data management

The nature of the IoT is dynamic and consists of different devices, sensors, platforms, and applications that operate across various networks. In addition, it generates, collects, stores, processes, and distributes huge amounts of data across different networks, which requires data management frameworks (Borgia, 2014; Padyab and Ståhlbröst, 2018; Gruen et al., 2002; Alam and Al Riyami, 2018). Thus, the IoT requires dedicated data management techniques that fit with its nature. This is because traditional database management techniques lag and may not satisfy the complex nature and needs of an IoT environment that can span global networks (Gruen et al., 2002; Husein, 2019). At present, most frameworks apply an integrated system for offloading data and information that conducts computationally intensive tasks on a worldwide cloud platform. Thus, several researchers have proposed some IoT data management frameworks for different purposes. Gruen et al. (2002) have developed a distributed data management scheme for storing data in an industrial IoT environment. Furthermore, (Gruen et al., 2002) provided a data management framework that focuses on three key functions of handling data: data collection, data storage, and data processing. Moreover, Rao and Shorey (2017) have developed a data aggregation model based on device-to-device data transmission. Another issue related to data management is the availability of data center technologies to manage data. According to Padyab and Ståhlbröst (2018), there is a greater need for different aggregate kinds of data generated by IoT sensors and devices in smaller, multiple, distributed data centers so that initial processing can be conducted to provide capture and response values in real-time. These include big data centers, distribution data centers, and micro data centers.

3.3. Machine-to-machine communication and messaging

The nature of the IoT requires constant communication between different kinds of devices and other communication systems, which is very challenging (Borgia, 2014; Alam and Al Riyami 2018). In addition, there is no standard for an open IoT communication protocol, which may further complicate the communication process (Husein, 2019). Communication protocols are key elements for IoT devices, sensors, and applications as they represent the main support for data flow and traffic among internal and external networks (Husein, 2019). Basically, research has been focussed on two broad categories related to M2M: The routing issues and the end to end reliability (Borgia, 2014). While several MAC protocols have been proposed for different types of domains with frequency division multiple access, carrier sense multiple access, and time division multiple access for small traffic competence that is accident-free, more integrated circuits in nodes are correspondingly essential (Husein, 2019). Borgia (2014) reviewed and discussed the M2M communications challenges in the context of the IoT thoroughly.

3.4. Interoperability

The interoperability issue has been widely reported in the IoT literature (Padyab and Ståhlbröst, 2018; Vermesan and Friess, 2013). In the IoT environment, interoperability among different kinds of data, networks, applications, and services is a requirement (Borgia, 2014; Díaz et al., 2016). The nature of the IoT is very complex, and interoperability is a key challenge (Gubbi et al., 2013; Borgia, 2014; Shin and Park 2017). This is due to the fact that IoT operation requires large and various devices at different levels; thus, it must have the ability to communicate and exchange data between these devices (Padyab and Ståhlbröst, 2018; Díaz et al., 2016). In general, there are four types of interoperability: Technical, syntactic, semantic, and organizational interoperability (Čolaković and Hadžialić, 2018). Another challenging issue is how interoperability can be achieved across legacy systems, achieving consistent integration and interoperability of virtual and real sensors (Vermesan and Friess, 2013).

3.5. Reliability, availability, and robustness

The reliability and availability of an IoT service is a significant challenge. It depends upon the consistency and obtainability of the communication. Nodes in the IoT might experience problems and failure for various reasons, including software bugs, limited energy, hardware failure, and malicious attacks. Thus, the reliability and robustness of services are an important and challenging issue (Alam and Al Riyami, 2018). The consequence of any loss of communication may be enormous financial fatalities, or it may even risk lives, in the case of Industry 4.0 and an intelligent transportation system, respectively. This problem may occur due to two reasons, either device failure or link failure. For link failure, there may be different solutions, but the provision of buffering or caching and the use of dynamic spectrum access are the prominent ones that can be pursued. In the case of device failure, redundancy in devices can be introduced. This calculation and placement must be done during the planning phase (Islam et al., 2015). The same solution can also help in the mobile maintenance of the services. The modern IoT as a challenge for higher education (Khan, 2018) is the acceptance of the IoT in the industry (the so-called Industry Internet of Things [IIoT]) and the requirements for higher education in the period of the fourth industrial revolution. 'IIoT' is similar to another term, 'Industry 4.0'.

3.6. Technological architecture issues

The IoT is still an evolving practice, and in order to utilize it effectively, there is a need to develop, maintain and integrate a robust technological architecture, including cloud computing, wireless technologies, artificial intelligent sensors, machine learning, blockchain, big data analysis techniques, server technologies, and data center technologies, which is very challenging (Borgia, 2014; Čolaković and Hadžialić, 2018; Alam and Al Riyami, 2018). IoT systems should be developed within open IoT technological architecture that ensures the integration of various technologies, mobility, scalability, interoperability, openness, and modularity in a heterogeneous environment and service continuity (Čolaković and Hadžialić, 2018). Overall, the technological architecture that needs to be addressed is related to general architecture, process architecture, software architecture, and hardware/network architecture (Whitmore et al., 2015; Čolaković and Hadžialić, 2018).

3.7. Standardisation

To improve the IoT's efficiency, it needs to rely on unified standards, and this is very challenging due to the difficulty in making one single standard for the IoT around the world (Whitmore et al., 2015). This is because the IoT is a complex system that requires the connection and interconnection of heterogeneous sensors, devices, actuators, software, systems, and networks, all of which have their own unique protocols to communicate, exchange and share data. Although there has been some progress regarding the development of some standards, for example, Open loT Stack for Java by Eclipse's foundation, the ongoing standardization initiative at ETSI and oneM2M, there is still a lack of common standards, which is one of the main challenges faced by the IoT (Padyab and Ståhlbröst, 2018; Aloi et al., 2017). According to Gubbi et al. (2013), key standardization bodies such as W3C, ITU, ETSI, IETF, IEEE, OneM2M, OASIS, and NIST are involved in the development of the IoT standards.

4. Conclusion

IoT is an emerging technology that promises to deliver unique services that will impact different aspects of our lives. The multifaceted nature of the IoT and its wide dependence on a large number of various devices, objects, technologies, and platforms has made it possible to be utilized in different domains and areas of contemporary society. This paper introduced a review of the possible applications of IoT and its associated challenges. It was intended to provide researchers and practitioners with some knowledge of the current thinking about this emerging topic (IoT applications and challenges). Since several governments around the globe have shown interest in the idea of the IoT by providing further funding to the topic that enables further investigation, several future research areas can be outlined. One possible area is how the IoT can be used in the different areas mentioned in this study.

Another research avenue could focus on one of the challenging issues associated with IoT adoption and utilization. Moreover, since IoT applications are a relatively new phenomenon, more research is needed to address how it can be applied in different areas of our lives, as well as researching challenges in different countries around the world, such as security and privacy issues, data management, machine-to-machine communication, interoperability, reliability and availability, technological architecture issues and standardization. Fig. 5 shows a summary of the prospects for utilizing IIoTs and their challenging issues.

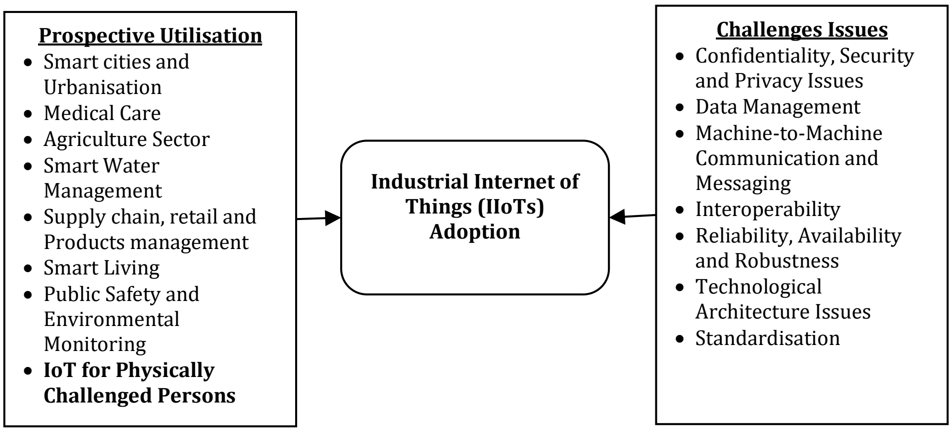

Fig. 5: A summary of the prospects for utilizing IIoTs and their challenging issues

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Ahlmeyer M and Chircu AM (2016). Securing the internet of things: A review. Issues in Information Systems, 17(4): 21-28.

Alam MA and Al Riyami K (2018). Shear strengthening of reinforced concrete beam using natural fibre reinforced polymer laminates. Construction and Building Materials, 162: 683-696. https://doi.org/10.1016/j.conbuildmat.2017.12.011

Aloi G, Caliciuri G, Fortino G, Gravina R, Pace P, Russo W, and Savaglio C (2017). Enabling IoT interoperability through opportunistic smartphone-based mobile gateways. Journal of Network and Computer Applications, 81: 74-84. https://doi.org/10.1016/j.jnca.2016.10.013

Borgia E (2014). The internet of things vision: Key features, applications and open issues. Computer Communications, 54: 1-31. https://doi.org/10.1016/j.comcom.2014.09.008

Cai H, Da Xu L, Xu B, Xie C, Qin S, and Jiang L (2014). IoT-based configurable information service platform for product lifecycle management. IEEE Transactions on Industrial Informatics, 10(2): 1558-1567. https://doi.org/10.1109/TII.2014.2306391

Chaudhary S, Johari R, Bhatia R, Gupta K, and Bhatnagar A (2019). CRAIoT: Concept, review and application (s) of IoT. In the 4th International Conference on Internet of Things: Smart Innovation and Usages, IEEE, Ghaziabad, India: 1-4. https://doi.org/10.1109/IoT-SIU.2019.8777467 **PMCid:PMC6807866**

Čolaković A and Hadžialić M (2018). Internet of things (IoT): A review of enabling technologies, challenges, and open research issues. Computer Networks, 144: 17-39. https://doi.org/10.1016/j.comnet.2018.07.017

Dagar R, Som S, and Khatri SK (2018). Smart farming–IoT in agriculture. In the International Conference on Inventive Research in Computing Applications, IEEE, Coimbatore, India: 1052-1056. https://doi.org/10.1109/ICIRCA.2018.8597264

Dastbaz M, Arabnia H, and Akhgar B (2017). Technology for smart futures. Springer, Berlin, Germany. https://doi.org/10.1007/978-3-319-60137-3 **PMid:29680604**

Dhanda SS, Singh B, and Jindal P (2019). Wireless technologies in IoT: Research challenges. In: Ray K, Sharan S, Rawat S, Jain S, Srivastava S, and Bandyopadhyay A (Eds.), Engineering vibration, communication and information processing: 229-239. Springer, Singapore, Singapore. https://doi.org/10.1007/978-981-13-1642-5_21

Díaz M, Martín C, and Rubio B (2016). State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing. Journal of Network and Computer Applications, 67: 99-117. https://doi.org/10.1016/j.jnca.2016.01.010

Dixit R, Malaviya D, Pandiyan K, Singh UB, Sahu A, Shukla R, and Paul D (2015). Bioremediation of heavy metals from soil and aquatic environment: An overview of principles and criteria of fundamental processes. Sustainability, 7(2): 2189-2212. https://doi.org/10.3390/su7022189

Grønbæk I (2008). Architecture for the internet of things (IoT): API and interconnect. In the 2nd International Conference on Sensor Technologies and Applications, IEEE, Cap Esterel, France: 802-807. https://doi.org/10.1109/SENSORCOMM.2008.20

Gruen TW, Corsten DS, and Bharadwaj S (2002). Retail out-of-stocks: A worldwide examination of extent, causes and consumer responses. Grocery Manufacturers of America, Washington, USA.

Gubbi J, Buyya R, Marusic S, and Palaniswami M (2013). Internet of things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7): 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

Husein AH (2019). Internet of things (IoT): Research challenges and future applications. International Journal of Advanced Computer Science and Applications, 10(6): 77-82. https://doi.org/10.14569/IJACSA.2019.0100611

Islam SM, Riazul DK, and MD HK (2015). The internet of things for health care: A comprehensive survey. IEEE Access, 3: 678-708. https://doi.org/10.1109/ACCESS.2015.2437951

Kamienski C, Kleinschmidt J, Soininen JP, Kolehmainen K, Roffia L, Visoli M, and Fernandes S (2018a). SWAMP: Smart water management platform overview and security challenges. In the 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops, IEEE, Luxembourg City, Luxembourg: 49-50. https://doi.org/10.1109/DSN-W.2018.00024

Kamienski C, Soininen JP, Taumberger M, Fernandes S, Toscano A, Cinotti TS, and Neto AT (2018b). SWAMP: An IoT-based smart water management platform for precision irrigation in agriculture. In the Global Internet of Things Summit, IEEE, Bilbao, Spain: 1-6. https://doi.org/10.1109/GIOTS.2018.8534541

Khan S (2018). Modern internet of things as a challenge for higher education. International Journal of Computer Science and Network Security, 18(12): 34-41.

Kor AL, Yanovsky M, Pattinson C, and Kharchenko V (2016). SMART-ITEM: IoT-enabled smart living. In the Future Technologies Conference, IEEE, San Francisco, USA: 739-749. https://doi.org/10.1109/FTC.2016.7821687

Kumar S, Tiwari P, and Zymbler M (2019). Internet of things is a revolutionary approach for future technology enhancement: A review. Journal of Big Data, 6: 111. https://doi.org/10.1186/s40537-019-0268-2

Li S, Tryfonas T, and Li H (2016). The internet of things: A security point of view. Internet Research, 26(2): 337-359. https://doi.org/10.1108/IntR-07-2014-0173

Ma Y, Wu C, Ping K, Chen H, and Jiang C (2018). Internet of things applications in public safety management: A survey. Library Hi Tech, 38(1): 133-144. https://doi.org/10.1108/LHT-12-2017-0275

Mahmud SH, Assan L, and Islam R (2018). Potentials of internet of things (IoT) in Malaysian construction industry. Annals of Emerging Technologies in Computing, 2: 44-52. https://doi.org/10.33166/AETiC.2018.04.004

Miraz MH, Ali M, Excell PS, and Picking R (2018). Internet of nano-things, things and everything: Future growth trends. Future Internet, 10(8): 68. https://doi.org/10.3390/fi10080068

Padyab A and Ståhlbröst A (2018). Exploring the dimensions of individual privacy concerns in relation to the Internet of things use situations. Digital Policy, Regulation and Governance, 20(6): 528-544. https://doi.org/10.1108/DPRG-05-2018-0023

Rao S and Shorey R (2017). Efficient device-to-device association and data aggregation in industrial IoT systems. In the 9th International Conference on Communication Systems and Networks, IEEE, Bangalore, India: 314-321. https://doi.org/10.1109/COMSNETS.2017.7945392
PMCid:PMC5546205

Righetti F, Vallati C, and Anastasi G (2018). IoT applications in smart cities: A perspective into social and ethical issues. In the IEEE International Conference on Smart Computing, IEEE, Taormina, Italy: 387-392. https://doi.org/10.1109/SMARTCOMP.2018.00034

Shin DH and Park YJ (2017). Understanding the internet of things ecosystem: Multi-level analysis of users, society, and ecology. Digital Policy, Regulation and Governance, 19(1): 77-100. https://doi.org/10.1108/DPRG-07-2016-0035

Sodhro AH, Pirbhulal S, and Sangaiah AK (2018). Convergence of IoT and product lifecycle management in medical health care. Future Generation Computer Systems, 86: 380-391. https://doi.org/10.1016/j.future.2018.03.052

Soomro S, Miraz MH, Prasanth A, and Abdullah M (2018). Artificial intelligence enabled IoT: Traffic congestion reduction in smart cities. In the Smart Cities Symposium 2018, Manama, Bahrain: 81-86. https://doi.org/10.1049/cp.2018.1381

Tadejko P (2015). Application of internet of things in logistics–Current challenges. Ekonomia i Zarządzanie, 7: 54-64.

Veena S, Mahesh K, Rajesh M, and Salmon S (2018). The survey on smart agriculture using IoT. International Journal of Innovative Research in Engineering and Management, 5(2): 63-66.

Vermesan O and Friess P (2013). Internet of things: converging technologies for smart environments and integrated ecosystems. River Publishers, Gistrup, Denmark.

Villanueva FJ, Villa D, Moya F, Santofimia MJ, and López JC (2012). Internet of things architecture for an RFID-based product tracking business model. In the 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IEEE, Palermo, Italy: 811-816. https://doi.org/10.1109/IMIS.2012.59

Weber RH (2010). Internet of things–New security and privacy challenges. Computer Law and Security Review, 26(1): 23-30. https://doi.org/10.1016/j.clsr.2009.11.008

Whitmore A, Agarwal A, and Da Xu L (2015). The internet of things-A survey of topics and trends. Information Systems Frontiers, 17(2): 261-274. https://doi.org/10.1007/s10796-014-9489-2

Woznowski P, Kaleshi D, Oikonomou G, and Craddock I (2016). Classification and suitability of sensing technologies for activity recognition. Computer Communications, 89: 34-50. https://doi.org/10.1016/j.comcom.2016.03.006

Xu LD, Xu EL, and Li L (2018). Industry 4.0: State of the art and future trends. International Journal of Production Research, 56(8): 2941-2962. https://doi.org/10.1080/00207543.2018.1444806

Zhu Q, Wang R, Chen Q, Liu Y, and Qin W (2010). IoT gateway: Bridging wireless sensor networks into internet of things. In the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, IEEE, Hong Kong, China: 347-352. https://doi.org/10.1109/EUC.2010.58