Chapter 4
IoT Applications and Business Models

Syed Ahsan Raza Naqvi, Syed Ali Hassan, and Fatima Hussain

4.1 Introduction

The Internet of Things (IoT) provides a notion of sensors or "things" being connected anytime, anywhere. It is considered to be an extension of the Internet to the real world consisting of physical objects, and is often associated with such terms as "ubiquitous network," and "cyber physical system" [1]. All future advancements in the field of IoT are contingent on developments in microelectronics, embedded systems and network protocols.

This chapter aims to provide the reader an overview of some of the fields that IoT can potentially revolutionize in the years to come. It discusses how IoT can change the way we will travel along national highways, how everyday garments may 1 day become more than just pieces of fabric, how two-way communication will play a major role in future electric grids and how it is helping to preserve endangered species like rhinos. Along the way, we outline some hurdles faced by IoT developers and how information security will shape future IoT networks. The chapter closes with a summary of business models that vendors may follow as IoT devices become increasingly pervasive in the market.

S.A.R. Naqvi
The University of Alabama, Tuscaloosa, AL, USA

S.A. Hassan
School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan

F. Hussain (✉)
Assistant Professor, School of Computer Science, University of Guelph, Guelph, ON, Canada

Research Associate, Department of Computer Science, Department of Electrical and Computer Engineering, Ryerson University, Toronto, ON, Canada
e-mail: fhussa03@uoguelph.ca; fatima.hussain@ryerson.ca

F. Hussain, *Internet of Things*, SpringerBriefs in Electrical and Computer Engineering, DOI 10.1007/978-3-319-55405-1_4

4.2 Applications of IoT

As will be seen in subsequent subsections, the applications of IoT are many and varied and the field has witnessed rapid growth in recent times. Therefore, in order to ease the development process of IoT applications, developers should move beyond low-level cloud programming models. In order to address this problem, [2] proposes a framework that is mapped to cloud application program interfaces (APIs) provided by platforms like Aneka. The framework not only reads data from both the sensors and online databases but also passes messages in case an event of interest is observed. The design is summarized in Fig. 4.1.

Generally, IoT is said to consist of the following layers [3]:

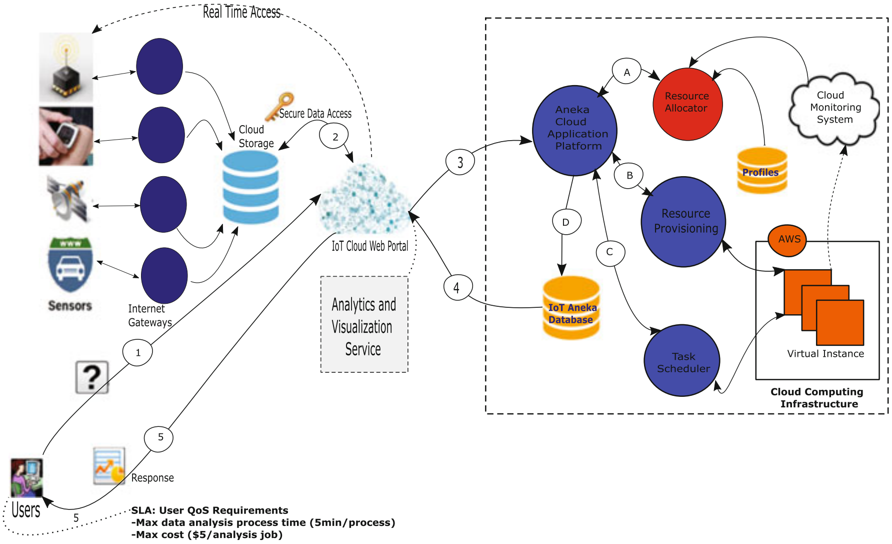

Fig. 4.1 Possible framework for developing future IoT applications

- Physical thing: It is the physical object, such as a light bulb, that provides direct benefits to the consumer.
- Sensor/actuator: The first layer is equipped with a minicomputer complete with sensors and actuators. The sensors are responsible for collecting data about the physical object and/ or its surroundings, whereas the actuator takes an appropriate measure in response to this data. For instance, a sensor might be used to determine whether or not there is human presence in the vicinity of a light bulb. Depending on this information, the actuator can turn the bulb either on or off.

(continued)

- Connectivity: The second layer is globally accessible through the internet to subscribers around the globe.
- Analytic: This layer collects and stores data originating from the sensors and checks for its plausibility.
- Digital service: The final layer packages the digital services offered by the previous layers in a suitable form.

4.2.1 Intelligent Transportation

It is expected that in the near future the principle of IoT could be applied to vehicles so as to set up car networks aimed at exchanging high rate multimedia information for entertainment purposes [4]. Such networks are called Vehicular Ad-Hoc Networks (VANETs). Device-to-device (D2D) communication is one of the promising applications of network control over communication sessions, whereby the devices discover each other and directly communicate with minimal involvement of the network. This strategy can help overcome latency issues in scenarios where vehicles communicate directly with each other, i.e., vehicle-to-vehicle (V2V) communication [5]. The resulting VANET converts the participating vehicle into a wireless router or node, allowing other cars within a proximity of 100–300 m of each other to connect and create a network. Vehicles moving out of this range are dropped from the network.

Vehicular communication is considered to be a front-runner in ensuring the security and the efficiency of future transportation systems by relaying information such as changes in the ambient conditions (snow, fire etc.) and traffic conditions in general (road accident, on-going construction work or congestion) (http://www.nautilus6.org/events/0701-WONEMO/20070115-WONEMO-Automotive.pdf). With each vehicle communicating in its neighborhood with unknown and unspecified vehicles on the road, V2V communication can prove to be vital for collision avoidance techniques as the distance and speed of the nearest neighbor is given greater importance in such situations.

There have already been other major developments towards achieving ‘smartness’ on the road. Multi-national enterprises around the world have made locating parking slots easier through sensors (ParkSight [6]), allowed users to summon cabs through a single tap of a smartphone (Uber [7]) and designed a mechanism for volunteers to collect road condition data for visualization on a map to be used by

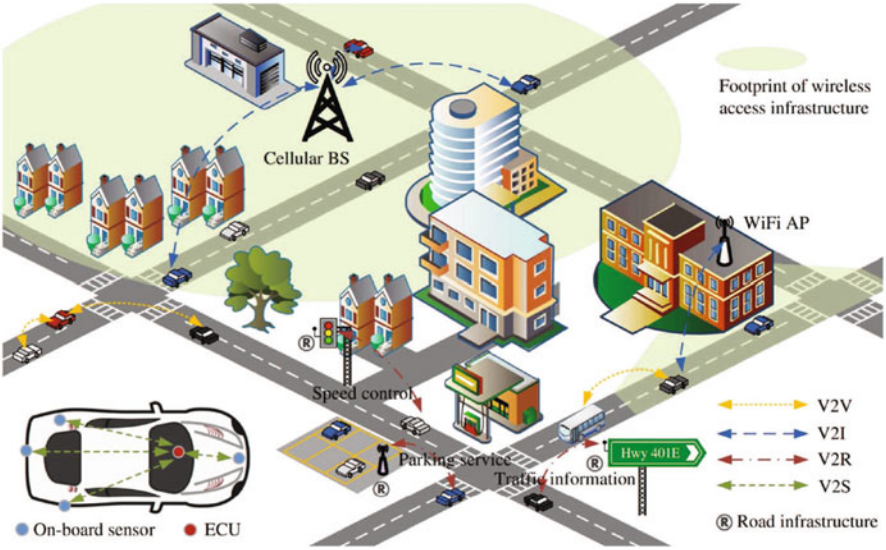

Fig. 4.2 Communication techniques expected to be used in VANETs comprising vehicles equipped with on-board sensors and electronic control unit (ECU); vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-road side unit (V2R) and vehicle to sensors (V2S) (https://ece.uwaterloo.ca/~kan.yang/securitybbcr/vanet.html)

both individual users and the authorities (Streetbump [8]). Needless to say, IoT is expected to continue playing a major role in determining how drivers interact with the environment, including the traffic, around them. Figure 4.2 summarizes the various communication techniques expected to be used in VANETs.

4.2.2 *Smart Clothing*

The state-of-the-art for smart clothing is restricted to special purpose, low-volume fabrics that are embedded with electronics. Related literature, however, projects the use of IoT in future garments by incorporating sensing layers, such as a conductive coating or a mesh of conductive threads, into a cloth during production. In particular, [9] lays down three requirements for achieving this:

- The sensor layers need to be tailored depending on what variables they aim to sense and the body location they are supposed to perform their job on.
- There should be a connectivity between the sensor layers to furnish a power and communication infrastructure for the sensory components.
- There should be an interface to set up the cloth to be embedded with electronic circuitry.

In conjunction to the aforementioned features, a separate operating system may be added to the electronic control modules.

IoT can also find application in product inspection and quality control. For instance, [10], proposes the design of a garment hanger that not only checks the appearance of the cloth (such as color and fitting) so that it meets predetermined standards, but also determine its tensile strength as well as its response to being worn by a person several times.

Researchers have also looked into the possibility of developing a sensor system to determine the optimal temperature for a building's heating or cooling system depending on the clothing insulation of the occupants [11]. The work was undertaken to prevent wastage of energy as well as reduce the feelings of discomfort experienced by people inside the building owing to inordinately high or low temperature settings. A smart sensor system for clothing insulation inference (SiCILIA) is a platform that addresses these challenges by obtaining the personal and physical variables of the inhabitant's thermal environment to deduce their clothing insulation.

4.2.3 Smart Grids

Earlier, the functionality of smart meters was restricted to measuring the electricity used and the ability to remotely control the supply and cutoff when necessary. However, the prospects of incorporating IoT principles into future electric grids have meant that smart meters will be able to perform a more diverse set of operations in the smart grid. These include, but are not limited to, real-time determination of electricity consumption with the possibility of remote and local reading of the meter, linkage with other utilities such as gas and water supply and recording events such as device status and power quality [12].

It would be instructive to note that while the smart meter is taken to be the data capture device, it may be connected to a communication device such as a smart meter gateway for setting up a secure network. This gateway could receive and communicate real-time information from the supplier and even start and stop power supply.

In addition, this gateway could also be connected to household appliances and is responsible for relaying consumption information to the subsequent level in the smart grid. In the long term, it has also been suggested that smart meters will also replace the large number of sensors currently being used in the grid by relaying voltage and current measurements directly to an aggregation point, thus reducing cost [13]. In literature, several communication techniques have been considered

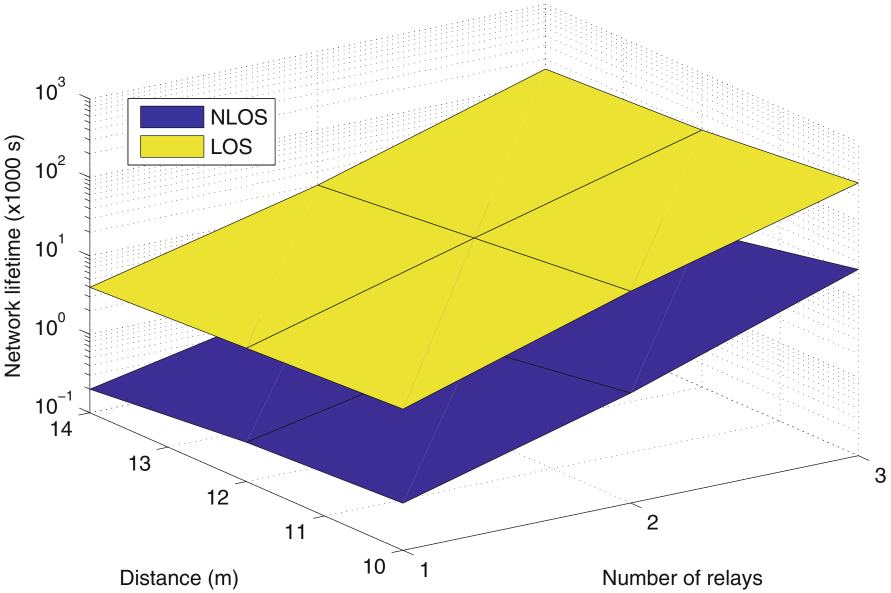

Fig. 4.3 Trade-offs between the number of cooperating relays, coverage distance and network lifetime

for use in transmitting this information in the neighborhood area network (NAN) of a smart grid. For instance, [14] develops a test bed using software defined radios (SDRs) to relay data from a source node, to multiple relays and then on to the destination node using cooperative communication. The setup has been tested in both indoor and outdoor environments. The paper showed that increasing the number of relays not only helped improve the coverage distance to achieve the same quality-of-service (QoS) but also offered better network energy efficiency as compared to systems that do not employ cooperative communication. Figure 4.3 illustrates one of the findings of the paper. The graph provides credence to the claim that increasing the number of relays to achieve the same QoS helps increase the network lifetime. This result is especially important considering the fact that most, if not all, sensors in an IoT network run on battery.

In addition to this work, [15] develops a media access control (MAC) protocol for such a network. Figure 4.4 outlines one set of results obtained by the authors. The figure shows the variation in throughput for increasing source-destination (S-D) distances at different transmit powers for single-input single-output (SISO) and cooperative links. An important observation from the plot is that the throughput performance of a cooperative network with a source transmit power of 5 dBm is comparable to that of a SISO network with a transmit power of 10 dBm.

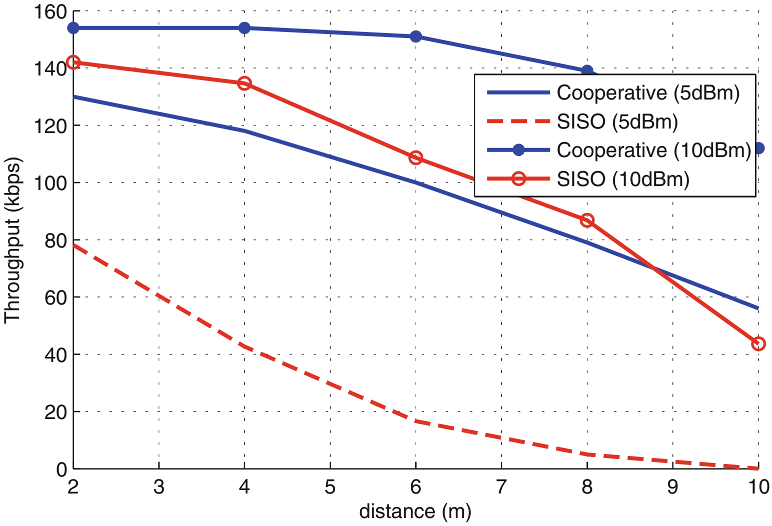

Fig. 4.4 Throughput versus S-D distance for SISO transmissions and CT

4.2.4 Education

With the vast proliferation of internet access, students and researchers now feel the urge to not only access the work of experts in their field but also their peers. The Internet has thus become a platform for sharing ideas and on-going research. It is expected that in the future experts in a particular area will be requested to teach classes anywhere in the world through streaming or live video [16].

Global education received a major boost with the introduction of massive open online courses (MOOCs). With the world's leading universities providing access to their professors free of charge, the idea of "flipped classrooms" is gaining strength, whereby students would be expected to learn the subject matter *outside* the classroom, leaving the course instructor to discuss problems and ideas during class time. By providing an opportunity for students in the developing world to learn beyond basic education (which is often limited by the economic status), MOOCs and other online resources like the Khan Academy [17] can, in time, help improve the quality of life for people who cannot afford higher education. Another major group of beneficiaries would be home-bound individuals who are capable of learning and participate in classroom courses.

In the future, MOOCs may transform into vehicles for two-way information which can prove vital for the universities and teachers engaged in furthering these initiatives. MOOCs can generate data-sets outlining the number of registrations and drop-outs, online attendance per course and the students' internet protocol (IP) address of the students. The universities can thus gauge the time that people spend on course materials and narrow down the content and topics that might be popular among specific demographics. This would allow course instructors to streamline their teaching methods to reduce drop-out rates and to align the curriculum to the students' needs.

4.2.5 Environment Observation, Forecasting and Protection

With the environment under constant stress due to extensive urbanization and adverse human activities such as hunting for sport, IoT is projected to play a part in preserving natural resources and endangered species. In order to achieve the latter objective, organizations around the world are using GPS-enabled devices to track the habits and health of endangered species (http://industrialiot5g.com/20161118/channels/fundamentals/iot-impact-environment-tag31-tag99). In fact, Cisco is using long range radio (LoRa)-based connectivity to track the movement of anyone entering the reserve grounds for rhinos (http://www.cisco.com/c/m/enus/never-better/csr-1.html). In case of trespassing, precautionary measures may be taken for the well-being of the animals.

Furthermore, IoT can potentially help alleviate waste management issues particularly in countries like the USA where the daily per capita trash was estimated to be 4.6 pounds in 2013 [18]. By determining the optimum time for waste collection and the best routes for the trucks to follow, IoT can redress the problems associated with waste build-up in neighborhoods.

With an increasing number of water-stressed countries around the world, the installation of smart water sensors in buildings can also help limit domestic water consumption. Through these devices and data analytics, users will be able to keep track of how much water was used in a given period, allowing them to cut down on excessive usage.

Another major environmental crisis that the world faces is deforestation. In addition to fighting forest fires, drones are now part of an initiative by BioCarbon Engineering to replant one billion trees [19]. The organization aims to achieve its goals through precision agriculture techniques, the use of technology to reduce manpower requirements and cost and the deployment of drones to determine the landscape of the area affected by deforestation.

Finally, IoT can also assist in predicting and mitigating the effects of natural disasters. In particular, Zizmo [20] uses cloud connected sensors that detect motion near earthquake epicenters to issue a warning to residents in the surrounding areas. Similarly, Avatech [21] uses pressure sensors to predict the likelihood of an avalanche.

4.2.6 Smart Agriculture and Farming

As stated earlier, the world's water reservoirs are fast depleting and there is an urgent need to conserve this precious resource. According to an estimate, farmers use 70% of earth's freshwater, 60% of which is lost due to faulty irrigation systems, inefficient agricultural techniques and the cultivation of thirsty crops (http://industrialiot5g.com/20161118/channels/fundamentals/iot-impact-environment-tag31-tag99). Sensors and actuators can provide growers with a better visibility over their operation and thus allow them to minimize water wastage by monitoring metrics such as temperature and water pressure. In this respect, Microstrain [22] has developed a system of wireless sensors to gauge key conditions during the growing season in vineyards. The sensors measure variables such as temperature, soil moisture and solar radiation and alert the farmers in case of extreme conditions. Figure 4.5 spells out the possible applications of IoT in farming.

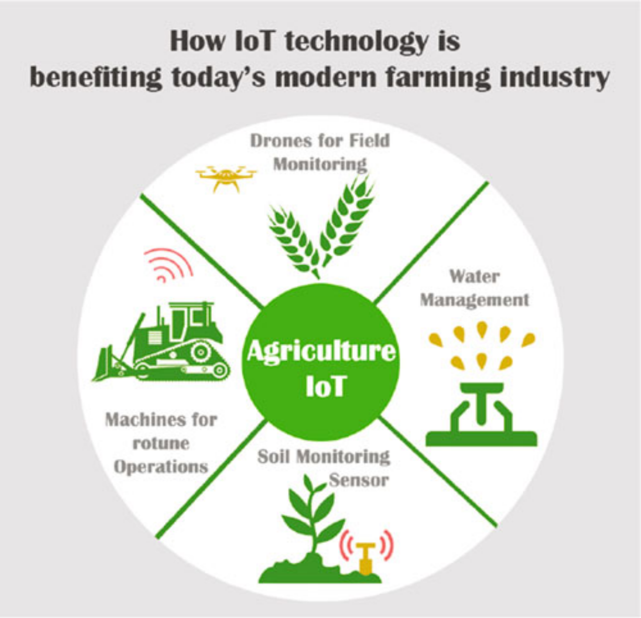

Fig. 4.5 Applications of IoT in agriculture (https://blog.beaconstac.com/2016/03/iot-ecosystem-iot-business-opportunities-and-forecasts-for-the-iot-market/)

4.2.7 Health Care

Given the vast number of future applications of IoT, it is little wonder that IoT is expected to revolutionize health care as well. In particular, IoT can allow physicians to constantly monitor the physiological parameters of their patients. Owing to the recent advances in wireless sensor networks (WSNs) and embedded systems, miniaturized health monitoring devices have become a reality. These sensors can form a body sensor network (BSN) which not only monitors the patients' health indicators but also incorporates context aware sensing for improved sensitivity. In this connection, [23] proposes the design of a hardware development platform.

The diagnosis of cardiac diseases by constantly monitoring the patient's electrocardiogram (ECG) signals is a common application of BSNs. These sensor networks have also been used for monitoring patients with Parkinson's disease as they offer credible data collected over a larger period of time, compared to the inferences made through clinical observation. For example, in [24], the authors used wearable sensors to identify the movement characteristics of patients suffering from Parkinson's disease and attained real-time monitoring with high accuracy. Similarly BSNs have also been used for the treatment of respiratory diseases. In such a scenario, the network comprises a respiratory sensor for determining the depth and frequency of breathing. The collected data might then be used for patients to undergo breathing training which is instrumental in respiratory disease rehabilitation. The setup includes It utilizes a respiratory sensor for monitoring depth and frequency of breathing, so as to guide patients to take correct breathing training, which plays a very important role in respiratory disease rehabilitation [25, 26]. Figure 4.6 summarizes the different components of a BSN.

4.2.8 Smart Homes/Buildings and Monitoring

Sensors can prove useful in preventing possible health hazards at home. For instance, environmental sensors can now monitor air quality, barometric pressure, carbon monoxide concentration, color, gas leaks, humidity, hydrogen sulfide levels and temperature, with upcoming start-ups offering users to access these details remotely. Netatmo [27] is one such venture. Other enterprises have tried to incorporate IoT principles to household lighting. Meethue [28], for example, is a bulb that can be controlled by mobile devices that is sensitive not only to the weather but also to user preferences, time and room activity. Additionally, some smart home solutions have also focused on facilitating the activities of the elderly. For instance, Ubi [29] a voice-activated computer allows access to an audio calendar, podcast and voice memos, and can also make lighting-based notifications to indicate the occurrence of certain events [30].

IoT principles have also been put to use to ensure building safety. Certain start-ups have developed sensors that can be embedded into the foundations allowing

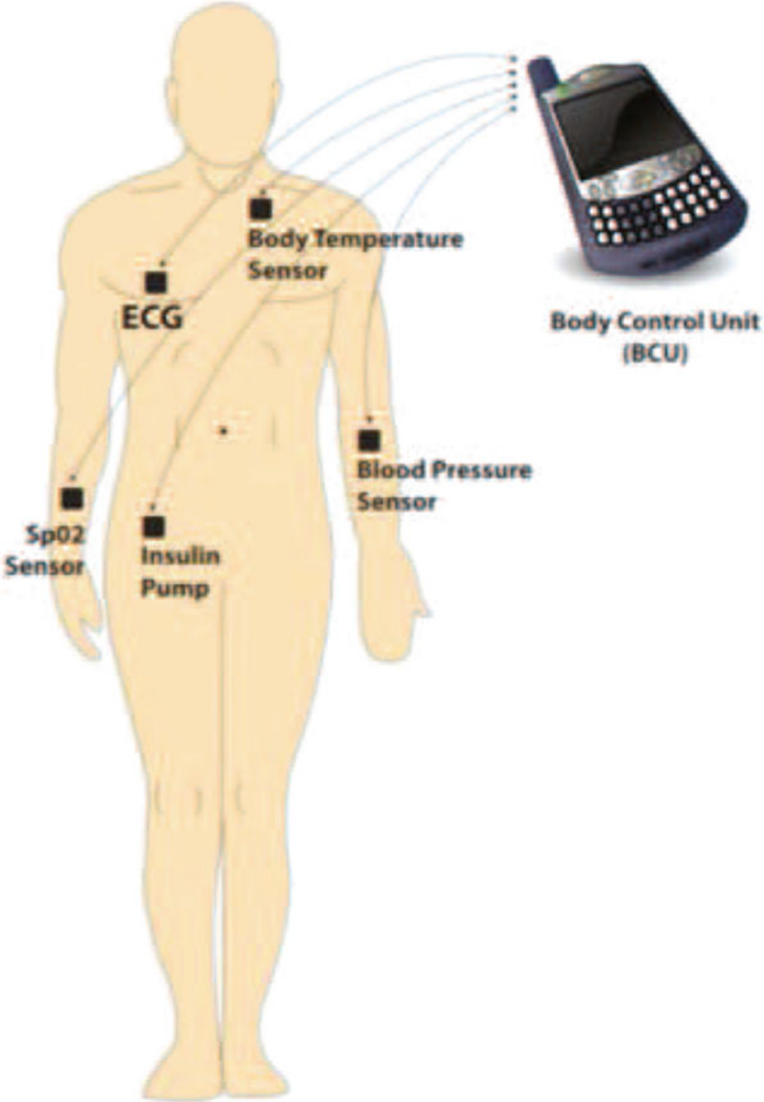

Fig. 4.6 Components of BSN (https://www.elprocus.com/ban-body-area-network/)

for consistent load monitoring, as well as those that can be used to maintain lifts and heating systems. Moreover, certain remote fire extinguisher monitoring systems have been developed which alert the user in the event of the fire extinguisher being absent from its designated position or its pressure falling below safe operating levels.

4.2.9 Public Safety

One manner in which IoT can facilitate public safety is through D2D communication [31]. Massive deployment of devices could help in multi-hop communication between the source and destination. Most of these devices utilize battery power so the network devised for disaster scenarios must be energy efficient. In post disaster scenario several of the devices are damaged and hence are unable to support the communication. The owners of the hand held devices can block any outside control thereby hindering the transmission. Viewing the sensitivity of the information in disaster and terrorism scenarios, the blockage of transmission is not affordable. The network needs to be resilient and be able to self-organize in case of any such situation. Similarly, several nodes might not be available for transmission due to low battery power. If the nodes reconfigure transmission protocols automatically there is a fair chance that the information is delivered to the destination. In case of disaster scenarios a "disaster mode" could be activated which is based on special routing for low power transmission and avoids any unwanted communication between devices. IoT has also been projected to play a major role in crowd management [32].

4.3 Research Challenges

Although IoT has opened up many exciting avenues for future development, researchers continue to grapple with roadblocks obstructing its expansion. This section will aim to delineate some of these challenges.

4.3.1 Versatile Sensors and Technologies

The first challenge deals with the sheer number of disparate sensor nodes, which cause a sensor network employing IoT to become a very complex heterogeneous network. With a wide array of networks employing several different communication techniques, IoT-based systems lack a common platform to provide a transparent naming service [33]. In addition, given the volume of data being transmitted the system frequently encounters latency and other communication issues [34]. The development of network protocols to ensure the smooth movement of data obtained from many different sensing devices within an IoT-enabled system is a major research challenge in itself. Modularity is also a key feature of IoT networks [30]. It refers to the concept of consumers building a smart object of their own without being restricted to products from a single vendor.

4.3.2 Integration of IoT and Conventional IT

There is also a need to combine IoT with conventional information technology (IT) systems to form a unified information structure. Integrating IoT devices with extant software systems would also demand the development of middleware. Furthermore, the large number of sensors that make up an IoT network produce large amounts of real-time data that may not be readily useful to the end consumer. The end-users would have to possess strong big data skills to make sense of the available information, which could be very challenging in itself.

4.3.3 Standardization

Another problem that needs to be looked into is standardization, which is aimed at improving interoperability of different application which in turn enhances performance. The new IoT standards should allow different types of sensors manufactured in various countries to exchange information [35]. In addition they should not only address radio access level and security issues [36–38], but also offer modifications that fit the needs of particular industries as well.

4.3.4 Security Protocols

One of the most crucial aspects of standardization in IoT is the development of security protocols to ensure privacy protection. The dependence of IoT networks on the cloud server makes such systems susceptible to cyber attacks. The current provisions for information security in IoT networks do not necessarily meet the strict requirements of certain industrial applications. Developing an encryption technology for IoT networks is expected to be more challenging than in the case of WSNs as the former allows several daily “things” to be connected and monitored, collecting a large volume of private data over a considerable period. One situation in which information security is essential is the case of self-driving cars of the future. These cars would be able to use VANETs to exchange, for example, data about distance and speed to avoid collisions. However, a malignant cyber attack on such vehicles could cause false data to be generated, putting lives at risk. Another scenario could include a BSN communicating a patient’s physiological parameters to a physician. In the absence of reliable security protocols, there is a possibility of the patient’s data being compromised, breaching doctor-patient confidentiality.

4.4 Business Models

A business model is defined as the plan implemented by a company to generate revenue and make a profit from operations (http://www.investopedia.com/terms/b/businessmodel.asp).

Given the nature of the IoT ecosystem, organizations not only have to collaborate with the firms from other industries but also their own competitors [39], which means that conventional business models are not applicable to the IoT phenomenon.

The authors in [40] stated that the current challenges of IoT include the vast number of connected objects in such networks, the fact that recent IoT innovations are yet to be tailored into products and services and a lack of clarity regarding the structure, governance and stakeholder roles in this emerging field.

Different frameworks of IoT related business models have been investigated in literature. For instance, [41] presented a 'D(esign) N(eeds) A(spirations)' model for IoT businesses, with 'design' referring to the key components of the system (including resources and activities), the 'needs' being customer relationship and 'aspirations' being the end result desired by the business e.g. revenue.

One of the unique features of IoT services is that customer behavior and feedback can be monitored consistently allowing businesses to incorporate newer features into the product. Thus, IoT bears the concept of service-dominant business model.

The model could also be used for effective forecasting and process optimization [42]. In this service-dominant business model [43], customers and firm are considered to be partners in the value creation process, in contrast to conventional models that project the latter as the sole value creators. The service-dominant model is an example of a network-centric view in IoT business which has been elaborated upon by [44] by proposing a service-based business model. The key elements of this model, along with associated issues, are summarized in Table 4.1.

Furthermore, authors in [3] also formulates a business model specific to IoT, consisting of six components listed in Table 4.2, terming the model as *Digitally charged products*. The paper describes physical freemium as some physical asset which is sold along with a free digital service, say digital installation and maintenance instructions, at no additional cost. Digital add-on refers to customers acquiring added services on top of what is offered by the product. These "add-ons" may be provided by the original vendor or by any third party enterprise. Digital lock-in

Table 4.1 Service based business model parameters [44]

Value proposition	Articulated offering
	Visualization
	Closer customer interaction
	A dynamic offering portfolio
Revenue mechanisms	New revenue model
Value chain	Dedicated roles for service development
	A structured service development process
	A new reward system
	Extending the resource base
Value network	Finding partners that can add value to the new offerings
	Competitive strategy
	Branding
	Differentiation
	Target market
	New customer segmentation

Table 4.2 Components and business model pattern in IoT [3]

Business model pattern	Components
Digitally charged products	Physical freemium
	Digital add-on
	Digital lock-in
	Product as point of sales
	Object self service
	Remote usage and condition monitoring

refers to a sensor-based, digital handshake which not only prevents counterfeits but also helps ensure warranties. The consumer pointing their smartphone at a product and accessing a web-site selling the same product, including accessories, is an example of products becoming points of sale. Object self-service refers to “things” serving themselves, such as a heating system ordering an oil refill when needed. Finally remote usage and condition monitoring refers to the constant connectivity of sensors to the internet where they upload real-time data which can be used to take corrective action in the case of an unusual event.

4.5 Conclusion

In this chapter, we aimed to summarize how IoT devices are changing the way we live and interact with the physical world. As IoT networks become increasingly complex and widespread, businesses around the world would have to rethink the process of value creation. Despite lingering concerns such as information security, it is safe to state that IoT can potentially bring about economic development which could be at par with that witnessed during the Industrial Revolution.

References

1. Zheng, L., et al., (2011). Technologies, applications, and governance in the internet of things. In *Internet of things-Global technological and societal trends: From smart environments and spaces to green ICT*. River Publisher series in Communication.
2. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.
3. Fleisch, E., Weinberger, M., & Wortmann, F. (2014). Business models and the internet of things. In *Bosch IoT Lab White Paper*.
4. Boeglen, H., Hilt, B., Lorenz, P., Ledy, J., & Poussard, A. (2011). A survey of V2V channel modeling for VANET simulations. In *8th International Conference on Wireless On-Demand Network Systems and Services, Bardonecchia* (pp. 117–123).
5. Nshimiyimana, A., Agrawal, D., & Arif, W. (2016). Comprehensive survey of V2V communication for 4G mobile and wireless technology. In *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), India* (pp. 1722–1726).
6. ParkSight: The complete smart parking solution, Streetline, Inc., Foster City, CA, USA, Tech. Rep., 2016.
7. Uber. (2016). *Uber* [Online]. Available: https://www.uber.com/
8. All Traffic Solutions. (2016). *All Traffic* [Online]. Available: http:/www.alltrafficsolutions.com/smartapps-video/smartapps-overview/
9. Cheng, J., et al., (2013). Smart textiles: From niche to mainstream. *IEEE Pervasive Computing, 12*(3), 81–84.
10. Wong, Y., & Ip, K. (2010). A three in one smart garment hanger. In *International Conference on System Science and Engineering, Taipei* (pp. 50–55).
11. Shaabana, A., Zheng, R., & Xu, Z. (2015). SiCILIA: A smart sensor system for clothing insulation inference. *IEEE Global Communications Conference (GLOBECOM), USA* (pp. 1–6).
12. Gerwen, R., Jaarsma, S., & Wilhite, R. (2006). *Smart Metering. Leonardo Energy (White Paper)* [Online]. Available: http://www.leonardo-energy.org/sites/leonardo-energy/files/root/pdf/2006/SmartMetering.pdf
13. Ilic, D., Karnouskos, S., & Da Silva, P. (2012). Sensing in power distribution networks via large numbers of smart meters. In *Proceedings of the 3rd IEEE PES International Conference and Exhibition on Innovative SmartGrid Technologies (ISGT'112)* (pp. 1–6).
14. Omar, M. S., et al., (2016). An experimental evaluation of a cooperative communication-based smart metering data acquisition system. *IEEE Transactions on Industrial Informatics, PP*(99), 1–1.
15. Amin, S., et al., (2016). Implementation and evaluation of a cooperative MAC protocol for smart data acquisition. In *IEEE 83rd Vehicular Technology Conference (VTC Spring), China*.
16. Selinger, M., Sepulveda, A., Buchan, J. (2013). Education and the internet of everything: How ubiquitous connectedness can help transform pedagogy. *Education IoE Whitepaper, Cisco*.
17. Khan Academy. *Khan Academy* (2016). [Online]. Available https://www.khanacademy.org
18. Report on the Environment (2013). *United States Environmental Protection Agency* [Online]. http://www.epa.gov/roe/
19. BioCarbon Engineering: Industrial scale reforestation services (2016). [Online]. http://www.biocarbonengineering.com/
20. Zizmos: Earthquake early warning system (2016). [Online]. https://www.zizmos.com
21. Avatech (2016). [Online]. http://avatech.com/
22. MicroStrain, Inc. (2016). *Shelburne Vineyard Remote Monitoring*. [Online]. Available: http://www.microstrain.com/news/shelburne-vineyard-relies-wireless-sensors-and-cloud-monitor-itsvines
23. Lo, B., Thiemjarus, S., King, R., & Yang, G. (2005) Body sensor network - A wireless sensor platform for pervasive healthcare monitoring. *Proceedings of 3rd International Conference Pervasive Computing* (pp. 77–80).

24. Patel, S., et al., (2006). Analysis of the severity of dyskinesia in patients with Parkinson's disease via wearable sensors. *Proceedings of the International Workshop on Wearable and Implantable Body Sensor Networks, USA* (pp. 4–126).
25. Mitchell, E., et al., (2010). Breathing feedback system with wearable textile sensors. In *Proceedings of the 2010 International Conference on Body Sensor Network (BSN), Singapore* (pp. 56–61).
26. Bates, A., et al., (2010). Respiratory rate and flow waveform estimation from tri-axial accelerometer data. *Proceedings of the 2010 International Conference on Body Sensor Network (BSN), Singapore* (pp. 144–150).
27. NetAtmo: Urban weather station (2014). Household Technol. PTY Ltd., Durban, South Africa.
28. *Meet Hue Personal Wireless Lighting*, Koninklijke Philips, Amsterdam, the Netherlands. http://www2.meethue.com/en-us/
29. Unified Computer Intelligence Corp. (2016). *UBI* [Online]. Available: http://theubi.myshopify.com/.
30. Perera, C., Liu, C. H., & Jayawardena, S. (2015). The emerging internet of things marketplace from an industrial perspective: A survey. In *IEEE Transactions on Emerging Topics in Computing, 3*(4), 585–598.
31. Huang, G., et al., (2016). D2D relaying based multicast service in Public Safety Networks. In *35th Chinese Control Conference (CCC), China* (pp. 6923–6927).
32. Kantarci, B., & Mouftah, H. (2014). Trustworthy sensing for public safety in cloud-centric internet of things. In *IEEE Internet of Things Journal, 1*(4), 360–368.
33. Miorandi, D., et al., Internet of things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497–1516 (2012)
34. Xu, L. D., He, W., & Li, S., (2014). Internet of things in industries: A Survey. In *IEEE Transactions on Industrial Informatics, 10*(4), 2233–2243.
35. Miorandi, D., et al., (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497–1516.
36. Wang, F., et al., (2013). A system framework of security management in enterprise systems. *Systems Research and Behavioral Science, 30*(3), 287–299.
37. Li, J., et al., (2013). A top-down approach for approximate data anonymisation. *Enterprise Information Systems, 7*(3), 272–302.
38. Xing, Y., et al., (2013). Operations research (OR) in service industries: A comprehensive review. *Systems Research and Behavioral Science, 30*(3), 300–353.
39. Chan, H. (2015). Internet of things business models. *Journal of Service Science and Management, 8*, 552–568.
40. Westerlund, M., Leminen, S., & Rajahonka, M. (2014). Designing business models for the internet of things. *Technology Innovation Management Review, 4*, 5–14.
41. Sun, Y., Yan, H., Lu, C., Bie, R., & Thomas, P. (2012). A holistic approach to visualizing business models for the internet of things. *Communications in Mobile Computing, 1*, 1–7.
42. Hui, G. (2014). How the internet of things changes business models. *Harvard Business Review, 8*, 552–568.
43. Turber, S., et al., (2014). Designing business models in the era of internet of things. In *9th International Conference DESRIST, USA* (pp. 17–31).
44. Kindstrom, D. (2010). Towards a service-based business model-key aspects for future competitive advantage. *European Management Journal, 28*, 479–490.