Noname manuscript No.
(will be inserted by the editor)

Internet of Things: Challenges and Research Opportunities

Md. Iftekhar Hussain

Received: date / Accepted: date

Abstract Fast development of sensor and network technologies is facilitating immense deployment of Internet of Things (IoT) towards creating a smart world. In IoT, a massive number of heterogeneous resource-constraint devices communicate with each other without any human intervention and generate a huge amount of data. Unique research challenges posed by IoT are fascinating the research community. This paper presents some of the critical issues along with state of the art solutions towards them. In-depth discussion is provided on various key issues like heterogeneity and interoperability, scalability, QoS, and security. Directions for further researches in those areas are also pointed out.

Keywords Internet of things · Scalability · Heterogeneity · Interoperability · Quality-of-Service

1 Introduction

Internet of Things (IoT) is the network of physical objects planted with sensors, actuators, RFIDs, software, and connectivity to enable it to interact with people and other connected devices in achieving some common goals ([39] and [36]). The number of devices connected in the IoT is increasing very fast. As such, it has been estimated that around 50 billion connected devices will be there by 2020 [15].

The devices used for sensing, actuating, and monitoring purposes are connected to the Internet by suitable communication technologies such as Wi-Fi, BLE, ZigBee, NFC, etc. In processing the huge amount of data generated and serving a large number of users in IoT, a cloud is essential. The cloud enables the applications to work anytime and from anywhere. The IoT applications are expected to work autonomously which can adapt and react intelligently over different situations, and support for easy integration. However, due to the wide heterogeneity and the resource-constraint nature of participating devices, these expectations remain as a challenge.

The integration of heterogeneous network systems have become the driving source of network alteration and has proposed various novel concepts such as Cloud of Things (CoT), Web of Things (WoT) and Social Internet of Things (SIoT) [42]. Thousands of IoT applications can be recognized in each domain and new ones emerging every day, requiring a strong Interoperability (IoP) among things. IoP further concerns various aspects such as security and privacy, standardization, etc. This brings new challenges driving research and innovation in industry and academia over the last decade. Accommodating a very large number of heterogeneous resource constraint devices in IoT also invites attention of research fraternity.

This article presents a holistic perspective on the IoT concept and development, enabling technologies, and critical research challenges. Considering the limited involvement of the networking and communications scientific communities in such an important development, I hope this work can boost more and more research in the highlighted issues and beyond.

The rest of the article is divided into following sections. Section 2 describes the background of IoT including its working principle and the protocol stack. Several critical research scopes and challenges along with their

Md. Iftekhar Hussain
North-Eastern Hill University
Tel.: +91-364-2723617
Fax: +91-364-2723606
E-mail: ihussain@nehu.ac.in

state of art are discussed in Section 3. Section 4 concludes the article.

2 Background of Internet of Things (IoT)

As the IoT encompasses a wide variety of concepts, a brief background of the IoT components is presented in this section.

2.1 What is IoT?

The basic idea of IoT is to equip the physical objects around us to sense the surrounding information, provide seamless communication and contextual services provided by them. The IoT is simply the network of interconnected things which are embedded with sensors, software, network connectivity, and embedded devices that enable them to collect and exchange data making them accessible over the Internet. IoT brings useful applications like home automation, smart health monitoring, security, automated devices monitoring, and management of daily tasks. Every sector like energy, computing, management, security, transportation are going to be benefited with this new paradigm.

IoT enables physical objects to see, hear, think and perform tasks by having them talk together, to share information and to coordinate decisions [5]. Development of sensors, actuators, smart phones, RFID tags makes it possible to materialize IoT which interact and cooperate each other to make the service better and make accessible at any time, from anywhere using any network. Wireless sensor technology allows objects to provide real-time environmental information and context. IoT allows objects to become more intelligent which can think and communicate among them.

In the vision of IoT, "things" are classified with three scopes: people, machine (sensor, actuator, etc.) and information (clothes, food, medicine, books, etc.) [1]. These should be identified at least by one unique way of identification for the capability of addressing and communicating with each other and verifying their identities. The identifiable "things" are known as "objects" in IoT. The major characteristics of IoT objects [40] are: (a) ability to sense or actuate, (b) small size, (c) limited capability, (d) limited energy, (e) connected to physical world, (f) intermittent connectivity, (g) mobility, (h) managed by devices, not people etc.

The scope of objects ranges from small to large. It is difficult to connect to power supply for the moving objects all the time. So they need to operate with a self-sustaining energy source. Therefore, energy efficient communication mechanisms are essential for IoT.

2.2 How it works?

IoT comprises of a wide variety of devices connected to each other with reference to their functional organization and configuration. An uniform standard architecture for all types of applications is desirable in order to support co-building and openness in IoT. Fig. 1 shows a typical architecture of IoT. The entire architecture is broadly classified into edge and platform tiers. The components of IoT in edge tier are the end devices (sensors, RFID, Camera, etc.), gateways, and sensor networks which are connected to the core via access networks. The platform tier contains the middleware, server and storage, and core services for device management, data management, real-time processing, analytics engines, and so on. A gateway is a device that has a short range of access link on one side, and a wide range of access link on the other side. It is a bit similar to our home router, which has a local network access towards our home computers and other IP-enabled devices, and WAN access toward our Internet service provider. The gateway node connects the two dissimilar networks that exist between IoT and Internet devices.

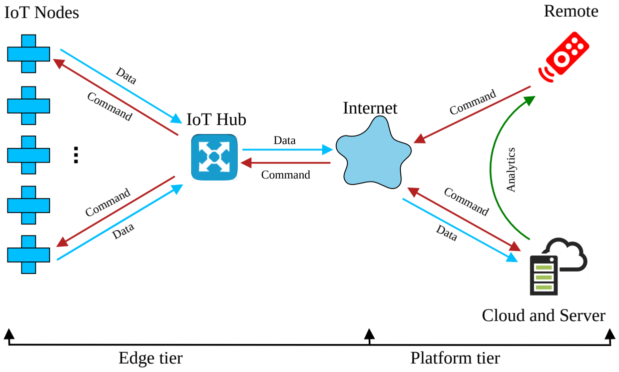

Fig. 1 A typical architecture of IoT

Sensors collect real-time data like video in case of intrusion detection system, audio or text in case of forest fire detection system. Router/Relay nodes work as forwarding nodes to transmit all the information associated with the different measured parameters. Both sensor and routers are configured to send all the information to the cloud or server. The sensor device can itself process the information and take action or it may send the collected information to the cloud through the Internet.

2.3 Protocol stack

The protocols required for effective communication in IoT can be positioned in a multi-layer stack as shown in Fig. 1. Primarily, data link, network, and application layer protocols are available in the literature. The protocols or technologies are mainly characterized by the light weight property but also focus on energy-efficient and scalable solutions for resource-constraint devices.

Table 1 IoT protocol stack

Layer	Protocols
Application Layer	CoAP [44], MQTT [19], SMQTT [33], XMPP [29], DDS [35], AMQP [38], IETF CORE, HTTP, SSH
Network Layer	6LowPAN [16], 6TiSCH [13], IPv4, IPv6 [29], RPL [41], CoRPL [4], CRB-RPL [43], IETF ROLL
Data Link Layer	802.15.4, RFID, 802.11g/ac/ad/ah [34], BLE [22], LTE-A [17], Z-Wave, NFC, ANT+ [45], LoRaWAN [7], SigFox [25]

Data link layer protocols are used to allocate channels or medium to stations for coordinating data transmission among smart devices. ZigBee [24] technology is based on IEEE 802.15.4 standard which is designed to provide a wireless data solution characterized by secure and reliable wireless network architectures. ZigBee is one of the most widely used protocol standards of IoT which enables smart objects to work together. The ZigBee devices are low latency devices and more responsive compared to Bluetooth devices as it takes only 30 ms to go from passive to active mode whereas Bluetooth takes approximately 3 seconds. BLE [22] is a short-range communication protocol that can save ten times more energy than classic bluetooth by using a contention-less MAC with low latency and fast transmission. The traditional IEEE 802.11 (Wi-Fi) standards are not suitable for IoT application due to its low scalability, frame overhead, and power consumption. The IEEE 802.11 working group started a task group to develop 802.11ah [34] standard which supports low overhead and power friendly communication which is suitable for IoT. To collect environmental information through sensors, IoT uses RFID reader in many cases. It is an identification technology that can automatically identify target devices and can collect data through its radio frequency signal without human intervention. It has the ability to uniquely identify the objects which are able to give the object location and can manage the correct communications and information processing.

The network layer protocols provide an abstract idea of the smart world devices. In addition to the traditional network layer protocols like IPv4 and IPv6 several new routing protocols such as 6LoWPAN [16], RPL [41], CoRPL [4], CRB-RPL [43] are proposed for IoT. To apply Internet protocol in such a huge number of resource-constraint devices, IPv6 [29] over 6LoWPAN [16] is preferred. Aiming to provide a suitable routing solution, the Routing Over Low power and Lossy Networks (ROLL) working group of the Internet Engineering Task Force (IETF) designed a new IPv6 Routing Protocol for Low power and Lossy networks (RPLs). It provides efficient routing paths for multi-hop mesh technologies in low power and lossy networks. RPL used link costs and node information as routing metric. Node information included available energy resources, workload, throughput, latency, reliability, and so on. The RPL is further modified in CoRPL [4] and CRB-RPL [43] which use Cognitive Radio (CR) for decision making.

In application layer, several new protocols are introduced to adapt with high volume and vast network of IoT devices. Machine-to-machine (M2M) communication Message Queue Telemetry Transport (MQTT) [19] is designed for IoT devices of small size that have low bandwidth, high cost, low processing power and unreliable networks such that they can communicate seamlessly among them. It provides a one-to-one classic M2M application in IoT. Some other suitable protocols are Constraint Application Protocol (CoAP) [44], Data-Distribution Service protocol (DDS) [35], Extensible Messaging and Presence Protocol (XMPP) [29], and Advanced Message Queuing Protocol (AMQP) [38]. CoAP is a web service oriented application which is designed to facilitate communication over resource-constraint electronic devices on the Internet. CoAP provides simplicity, low overhead and multicast support which can easily be translated into HTTP for simplification.

To provide human-to-human (H2H) communication in IoT, another XML-based instance message oriented protocol called XMPP [29] is proposed. It is designed to connect people to other peoples by instant messaging. The Data-Distribution Service (DDS) protocol [35] offers interoperability between IoT connected smart devices and provides scalability, performance enhancements for IoT applications. It supports multicast as well as multiple transport protocols such as TCP/IP and UDP/IP for providing high throughput and low latency. For its distributed processing nature it can directly be connected to sensors, smart devices without using any centralized server. Advanced Message Queuing Protocol (AMQP) [38] is designed for IoT which is mostly suitable for server-based analysis and control plane. It provides interoperability and reliability for the queuing messages between servers. AMQP also feasible for flexible routing, publish-subscribe messaging, transaction and security.

3 Challenges and Research Opportunities in IoT

As the IoT is the integration of heterogeneous technologies that are used to sense, collect, act, process, manage, transmit, notify, and store data, there are many research issues and challenges which have cropped up spanning several research areas. In this section, the key research issues and challenges are explained showing future research directions in each area.

3.1 Heterogeneity

Heterogeneity is one of the critical issues of IoT. Device heterogeneity can be in terms of different technologies, sensing, various software, and processing strategies used in IoT. In traditional computer environments, computer devices are treated equally when connected to the Internet. Their functionalities vary depending on how the users use them. However, when we talk about IoT, each device would be subjected to different conditions such as power consumption, processing capabilities, and communication bandwidth requirements [14]. The heterogeneity of IoT may be due to-

1. Operating conditions: The sensor devices operate in different conditions like- temperature, pressure, and voltage.
2. Functionality: The IoT devices may either deliver data periodically or on demand basis.
3. Resolutions: The objective of IoT devices may be tracking, monitoring, actuating, etc.
4. Hardware platform: The hardware platform varies according to their architecture and design. Based on this, the supporting operating systems and applications are also different.
5. Service pattern: The pattern of IoT services may differs in generation rate, packet size, etc.
6. Implementations: Different programming languages are used to develop IoT applications using different operating systems, such as Android, iOS, etc.
7. Interaction modes: The interaction between IoT devices and the remote user can be request/response or command type.

When a plethora of IoT applications towards improving quality of human life are being developed, various new devices, protocols, network connectivity methods and resulting application models are evolving. Sticking to single protocol standard in IoT is not an easy task. Moreover, even within one standardized protocol suite there are a number of different application domains and communication technologies available. Forcing IoT users to support these different types of diversity is not feasible as they typically lack the proper resources (e.g., know-how, time, and processing resources) to handle the specifics constrained devices and networks. To provide support for seamless communication among such heterogeneous devices, interoperable solutions are really required to be incorporated.

3.2 Interoperability (IoP)

In IoT, each device would be subject to different conditions such as energy constrained, communication bandwidth requirements, computation and security capabilities [37]. Things could be made by various manufacturers that do not necessarily follow the common standard. Moreover, devices may also operate using a variety of communication technologies. These technologies do not necessarily connect IoT devices to the Internet in the same way a typical computer device usually do. Fig. 2 explains a typical IoP scenario in the context of IoT. Here, various devices trying to communicate among them using heterogeneous communication technologies (RFID, Bluetooth, Wi-Fi, ZigBee, NFC, etc.). For example, a Bluetooth mouse cannot communicate with a laptop which is using Wi-Fi technology. To solve these issues we can use a smart gateway or IoT cloud to provide IoP among them.

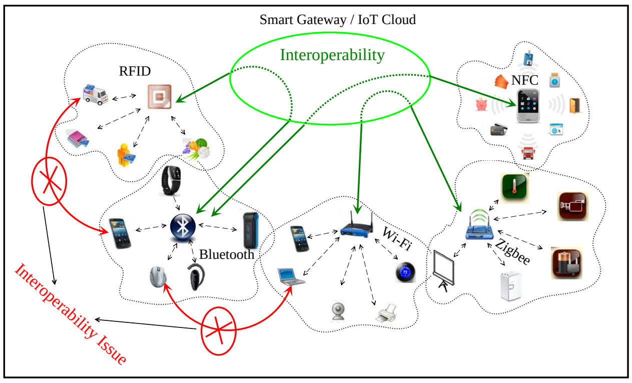

Fig. 2 A scenario of Interoperability issue in IoT

The heterogeneous devices which are broadly used in IoT need to talk and work together. To achieve this, different IoT systems need to be integrated. However, at the technical level, interoperability still represents a significant barrier. Up to 60% of the values that IoT systems might disclose is currently locked by a lack of interoperability [14]. As several heterogeneous systems need to communicate, IoT faces various IoP challenges before being able to create real domain services with seamless communication of devices and data.

Different categories of IoP issues are appearing in the context of IoT. Various types of IoP issues that are needed to be addressed in supporting seamless and heterogeneous communications in the IoT are shown in Fig. 3.

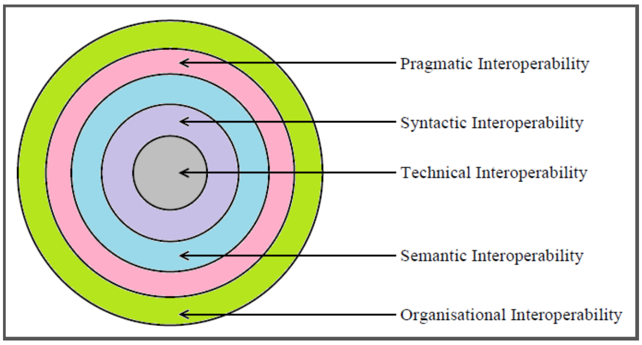
Pragmatic Interoperability
Syntactic Interoperability
Technical Interoperability
Semantic Interoperability
Organisational Interoperability

Fig. 3 Different levels of interoperability

1. *Technical Interoperability:* It is the incompatibility of the communication technologies and protocols that are used to exchange information. This type of interoperability provides only low level integration which guarantees the correct transmission of bits among different heterogeneous systems.
2. *Syntactic Interoperability:* It can be found whenever different people or systems use different structures and types to represent information and knowledge [3]. Syntactic interoperability is usually associated with data structures and formats (e.g., JSON or XML). Certainly, the messages passed over by communication protocols need to have an explicit encoding and syntax, even if it is only in the form of bit-tables. [37]
3. *Semantic Interoperability:* Semantic interoperability issue refers to having different meaning of the same content. Semantic Interoperability is mainly concerned with the human rather than machine-to-machine interpretation. It gives the meaning of the information which is being exchanged between them [12]. It is considered as an important barrier to providing interoperability as the information and knowledge represented in most of the software have not distinctly defined semantics to allow unambiguous understanding of the meaning of content.
4. *Pragmatic Interoperability:* It explains the unexpectedness about the effect of the exchanged messages and context between the sender and receiver. Pragmatic IoP provides the compatibility between the intended against the actual use of exchanged message within an appropriate shared context [28]. The approach of pragmatic interoperability is still largely unsettled, as illustrated by the various proposed definitions ([9], [8], [31]) and the lack of a authorized understanding.
5. *Organizational Interoperability:* Organizational Interoperability is the inability of organizations to effectively communicate and transfer meaningful information among them when they are using a variety of different information systems over widely different infrastructures, geographic regions and cultures. It depends on successful technical, syntactical, semantic and pragmatic interoperability. Organizational Interoperability is the ability of an enterprise, a company or other large organization to practical link activities, such as supply chains, product design, manufacturing, in a competitive and efficient way [10]. This makes sure that all industries maintain the same pattern of organization and makes it easier to manage multiple clients.

Achieving IoP among all the heterogeneous devices across various communication technologies is indispensable. It will defeat the very purpose of having billions of sensors, actuators and tiny smart devices connected to the Internet if they are actually unable to communicate with each other in any way. In fact, for the IoT to flourish, things connecting to the communication networks, which can be heterogeneous, need to be able to communicate with other things or applications. Some possible approaches to provide IoP are discussed below-

1. Protocol Translation: Gateway acts as proxies to convert proprietary protocols to TCP/IP and vice versa. It has low complexity, low-cost, and can easily be adopted. But due to lack of unified standards, protocol translation causes isolation among IoT applications.
2. IPv6 over WSN: IPv6 can be used in WSN by compressing the header and using the stateless autoconfiguration of IPv6. But, as IoT things are of different sorts and sizes, further efforts are still required to ensure that the proposed stack is adaptable to devices with different and limited capabilities.
3. Using Device Ontology: Using ontology, we can share the common understanding of the structure of information among people or software agents. It gives meta-information, knowledge and description about devices such as- device name, vendor details, hardware description and software description, etc. But, all device providers will not adopt the same set of ontologies because of their different contexts.

4. Web of Things (WoT): Here, every node in the network run a web server. The client is able to access any devices included in the network. The main limitation of WoT is that it is based on user-centric architecture. Here, actions done by devices are always initiated by a user.
5. Service Oriented Middle-ware (SOM): Data generated from the sensor devices are treated as services. The interaction between producer and consumer is done by the registry which provides discovery, managements, and access to the consumers. But, most existing SOMs are WSNs-centric and their scale is limited to WSNs, which is typically in the range of thousands, much less than the ultra large-scale (billions) of IoT.
6. Designing a Generic Protocol Stack: We can design a protocol stack by integrating all the other low power technologies which can be able to provide interoperability at different aspects such as- physical integration that focuses on interconnecting different devices, application integration executing different applications concurrently, etc. It supports all types of low-power radio hardwares (NB, HBC, and UWB).

3.3 Scalability

Scalability is the key to handling the explosive growth in the IoT. With the increasing number of nodes, all other components (as shown in Figure 4) are also increasing proportionally. The IoT applications must have the ability to support an increasing number of connected devices, users, application features, and analytics capabilities without any degradation in the QoS. Monitoring, securing, and managing an increasing number of devices require a proportionate increase in the resources.

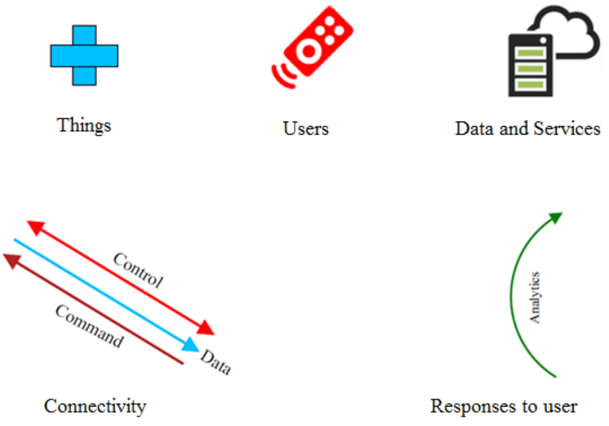

Fig. 4 Different components participating in IoT

As a massive number of connections are needed to be maintained by a cloud server with the deployed devices. Provisioning scalability in such architecture is a primary concern. Further, networking and communicating among such huge number of devices is another challenge of IoT. The scalable approaches to handle these challenges primarily lie in i) Cloud and server platform and ii) Network and communication protocol.

3.3.1 Cloud and server platform

When the number of devices grows, numbers of connections and data produced by these devices also grows. As such handling massive connections, data volumes, and request/response a big challenge. Some of the cloud solutions for IoT are openIoT[1] , Compose[2], ClouT[3], and Kaa[4]. Different strategies adopted to enhance scalability are:

1. To deal with the reliability issues, scheduling mechanisms need to be developed for maintaining duplicate services in case failure [21].
2. The services in a cloud should take the responsibility to enable automated bootstrapping, registration, monitoring, and upgrade.
3. A data processing pipeline is required to be developed for collecting, cleaning, enrichment, and transformation on streaming data [26].
4. Three dimensions- X, Y, and Z axes based scaling approach is very important to handle massive requests, actions, and data [6]. The X-axis scaling involves in dividing the requests among multiple servers. Y-axis approaches divide the workload based on actions. The incoming request data or the response data are carried out in Z-axis scaling approaches.
5. In order to scale an IoT application, it needs to break down into multiple independent functional units, each of which performs one dedicated function [26]. Each of these functional units should be independently deployable and executable.
6. It needs to adopt multiple data storage technologies. The query and retrieval requirements coupled with the analytics algorithms that run on the selected data, should determine the choice of data storage or the database technology [30].

[1] http://openiot.eu/
[2] http://www.compose-project.eu/
[3] http://clout-project.eu/home2/
[4] http://www.kaaproject.org/

3.3.2 Network and communication protocol

In the context of IoT communications, there may be thousands of devices which try to transmit simultaneously. For example, hundreds of Philips HUE lamps in a dense ZigBee network was shown at the 2014 Light and Building Fair in Frankfurt [11]. A large number of devices need to connect to a single network for a special objective. As such, networking and communication with limited channel bands is challenging. LTE-A [17], IEEE 802.11ah [2], and 6LowPAN [32] are some of the existing scalable solutions for MAC, PHY, and network layers. Different strategies for providing scalability are:

1. The physical layer techniques have greatly improved the link capacity in wireless networks. New modulation and coding schemes (MCSs) are required for improving network capacity.
2. With increasing number of active things in IoT, the Medium Access Control (MAC) protocols should be able to control contention and collisions over the shared wireless medium to deliver stable performances.
3. To uniquely identify the devices, the addressing schemes IPv4 and IPv6 are the solutions. The limited address space of IPv4 has driven the transition to IPv6. The IPv6 can give available unique and globally routable addresses. However, higher overhead in use of IPv6 is a great concern for such resource constraint networks.
4. Another important aspect of provisioning scalability is to minimize the protocol overhead as the network size and the physical layer capacity increases.
5. The devices are constraint in nature and it is very important that the protocols are optimized to consume very low power.
6. Data aggregation techniques are used to deal with the redundant data. It combines all the redundant and correlated data into valid high-quality information which is in turn transmitted to the sink through the intermediate nodes. This process can reduce the number of redundant packets transmitted.

3.4 Security and Privacy

Several new security and privacy challenges are introduced in IoT. Due to the resource-constrained nature of IoT devices, it is very difficult to protect the information. On the other hand, IoT requires global connectivity and accessibility; which means that anyone can access IoT devices at anytime and anyway. For that, the number of attacks available to malicious attackers might become overwhelming. Again, the communication between constrained devices and other entities depends on radio wave, which is susceptible to many attacks [20]. The indispensable complexity of the IoT, where multiple heterogeneous devices located in different contexts can exchange information with each other, further complicates the design and deployment of efficient, interoperable, and scalable security mechanisms. Cloud computing and the ubiquity also increases the urgency of the privacy leakage problem. As a result, there is an increasing demand for the development of novel security and privacy mechanisms to guarantee the security, privacy, integrity, and availability of resources in IoT.

Traditional security approaches cannot be directly used in IoT because of the different standards and communication stacks involved. Therefore, novel and new security and privacy methods and solutions are needed to deal with security threats in IoT. Some of the future research challenges are listed as follows-

1. Designing lightweight security solutions for resource-constraint networks and devices is an important task.
2. Universal authentication is a network identity verification method that allows users to move securely from one place to another without entering identifying information multiple times. The same can be applied in IoT.
3. Identifying individuals in a system (such as a country, a network, or an enterprise) and accordingly control their access to resources within that system by associating user rights and restrictions are very important.
4. Provisioning data availability by serving and protecting them in a cloud is one of the major issues of the future IoT. Some of the data protection solutions available in the literature are Commvault[5], NetBackup[6], Rubrik[7], and Veeam[8].
5. Privacy preserving services are also necessary in the context of IoT.

3.5 Quality of Service (QoS)

QoS provisioning in IoT applications has become a hot and unexpanded research topic in todays era. There are so many QoS challenges in IoT to be addressed like availability, reliability, mobility, performance, scalability, interoperability, security, management, and trust [23].

[5] http://www.commvault.com

[6] http://www.veritas.com/product/backup-and-recovery/netbackup

[7] http://www.rubrik.com

[8] http://www.veeam.com

Table 2 QoS requirements of various IoT applications

Application	Type of data flow	Delay sensitiveness	Priority	Availability	Reliability	Scalability
Health-care	Continuous	High	High	High	High	High
Environment monitoring	Event	Medium	Moderate	High	High	High
Smart Vehicle	Continuous	High	High	High	High	High
Smart Home	Event, Query	Medium	Moderate	High	High	Moderate
Children Monitoring	Continuous	Medium	Moderate	High	High	Moderate
Social Networking	Query	Low	Low	Low	Moderate	Moderate
Smart Traffic Control	Continuous	High	High	High	High	High
Smart Business	Continuous	Medium	Moderate	High	High	High

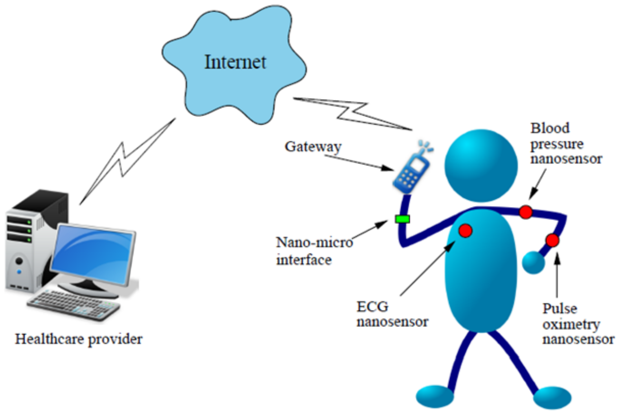

Fig. 5 An example of smart health-care system

In a smart health-care monitoring system (as shown in Fig. 5), it is necessary to constantly monitor the patients physiological parameters. For example, a pregnant woman parameters such as blood pressure and heart rate of the woman and heart rate and movements of fetal to control their health condition. This monitoring systems not only monitor vital signs but also detect abnormalities and transmit the data in real-time to health-care providers. In such a scenario, reliable delivery of those sensitive data to the service provider without compromising delay and accuracy is important. Hence, requirement of QoS for the IoT application is very much necessary to provide the services in some better and smart way. Many protocols are developed to provide QoS to various applications depending upon their types of services or their needs. Table 2 discusses several IoT applications and their required QoS parameters for seamless and better services.

Due to the architectural differences and a wide range of devices and networks involved in it, provisioning QoS in IoT is a very challenging task. The main challenges in provisioning QoS in IoT are as follows -

1. Resource-constraint devices: The sensor devices in IoT are placed in remote areas, so power constraints is a big issue in this case [27] . Besides this power constraints there are some other issues like bandwidth, buffer size, memory available, processing capability of the nodes.
2. Traffic load: The traffic load in IoT is unbalanced as the sink node is getting data from a large amount of sensors scattered in the environment. This unbalanced traffic load also effects in the overall QoS of a network.
3. Data redundancy: As already mentioned, the sink node receives data from a large number of sensor nodes. Among all these data, there will be some redundant data [18]. Sending this redundant data will cause wastage some extra amount of energy which will effect in QoS. Using some data fusion or data aggregation techniques the redundant data can be eliminated.
4. Scalability: Scalability is also an open issue for IoT applications. An application should work consistently even when some more users are added to the network.
5. Fault tolerance: Node failure or link failure is a big issue towards provisioning QoS in wireless networks.
6. Heterogeneity: Heterogeneity in IoT effects in QoS provisioning.
7. Multiple receiver and traffic types: Application wise there will be multiple receiver which needs different types of traffic model. This is also affect in the QoS in IoT.
8. Real time requirements: Multimedia applications like video chatting, texting, audio chatting shows different types delay sensitivities, which is very difficult to achieve as a whole.

Some of the possible solutions to provide QoS to several IoT applications are mentioned below:

1. Application specific QoS architecture.
2. Designing efficient MAC protocol to deal with energy efficiency, throughput, and delay.

4 Conclusion

Over the last few years, Internet has changed drastically. Due to the availability and the advancement of the sensor and cheap hardware technologies, it has been possible to attach sensors to all the physical devices around us enabling them to communicate with each other without human intervention. This article provided a brief understanding to the main concepts, protocol stacks and features of IoT. It analyzed the objectives and challenges of IoT technology by indicating some of the probable solutions. This work will help in providing the theoretical foundation for developing large-scale practical IoT systems.

References

1. The Internet of Things - Concept and Problem Statement(draft). `https://tools.ietf.org/html/draft-lee-iot-problem-statement-00`
2. IEEE Draft Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 11. IEEE P802.11ah/D6.0, (Amendment to IEEE Std 802.11REVmc/D5.0) pp. 1–645 (2016)
3. Ahsan, M., Talib, M.R., Sarwar, M.U., Khan, M.I., Sarwar, M.B.: Ensuring Interoperability Among Heterogeneous Devices through IoT Middleware. International Journal of Computer Science and Information Security **14**(4), 251–255 (2016)
4. Aijaz, A., Su, H., Aghvami, A.H.: CORPL: A routing protocol for cognitive radio enabled AMI networks. IEEE Transactions on Smart Grid **6**(1), 477–485 (2015)
5. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys Tutorials **17**(4), 2347–2376 (2015)
6. Aljawarneh, S.: Cloud Computing Advancements in Design, Implementation, and Technologies. IGI Global (2012)
7. Alliance, L.: Lorawan specification. LoRa Alliance (2015)
8. Asuncion, C.H., van Sinderen, M.: Towards Pragmatic Interoperability in the New Enterprise — A Survey of Approaches, pp. 132–145. Springer Berlin Heidelberg (2011)
9. Bravo, M., Velazquez, J.: Discovering Pragmatic Similarity Relations between Agent Interaction Protocols, pp. 128–137. Springer Berlin Heidelberg (2008)
10. Chen, D., Daclin, N., et al.: Framework for enterprise interoperability. In: Proc. of IFAC Workshop Enterprise Integration, Interoperability and Networking (EI2N), pp. 77–88. Standards Norway (SN) (2006)
11. Dandelski, C., Wenning, B.L., Perez, D.V., Pesch, D., et al.: Scalability of dense wireless lighting control networks. IEEE Communications Magazine **53**(1), 157–165 (2015)
12. Desai, P., Sheth, A., Anantharam, P.: Semantic gateway as a service architecture for IoT interoperability. In: 2015 IEEE International Conference on Mobile Services, pp. 313–319. IEEE (2015)
13. Dujovne, D., Watteyne, T., Vilajosana, X., Thubert, P.: 6tisch: Deterministic ip-enabled industrial internet (of things). IEEE Communications Magazine **52**(12), 36–41 (2014)
14. Elkhodr, M., Shahrestani, S., Cheung, H.: The internet of things: New interoperability, management and security challenges. arXiv preprint arXiv:1604.04824 (2016)
15. Evans, D.: The Internet of Things. How the Next Evolution of the Internet is Changing Everything, Whitepaper, Cisco Internet Business Solutions Group (IBSG) (2011)
16. G. Montenegro, N.K., Hui, J.: Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944, RFC Editor (2007). URL `https://tools.ietf.org/rfc/rfc4944.txt`
17. Ghosh, A., Ratasuk, R., Mondal, B., Mangalvedhe, N., Thomas, T.: LTE-Advanced: Next-generation Wireless Broadband Technology [Invited Paper]. IEEE Wireless Communications **17**(3), 10–22 (2010)
18. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems **29**(7), 1645–1660 (2013)
19. Gunner, B.: MQTT Will Enable The Internet Of Things (2013). URL `\url{https://www.ibm.com/developerworks/community/blogs/c565c720-fe84-4f63-873f-607d87787327/entry/tc\_overview?lan=en}`
20. Han, G., Shu, L., Chan, S., Hu, J.: Security and privacy in internet of things: methods, architectures, and solutions. Security and Communication Networks **9**(15), 2641–2642 (2016)
21. Hao, Y.F.S.J.J.: A Scalable Cloud for Internet of Things in Smart Cities. Journal of Computers **26**(3), 1–13 (2015)
22. J. Nieminen T. Savolainen, M.I.N., Patil, B.: IPv6 over BLUETOOTH(R) Low Energy. RFC 7668, RFC Editor (2015). URL `https://tools.ietf.org/html/rfc7668.txt`
23. Kaur, S., Mir, R.N.: Quality of service in wsn-a review. International Journal of Computer Applications **113**(18) (2015)
24. Lin, M.S., Leu, J.S., Li, K.H., Wu, J.L.C.: Zigbee-based internet of things in 3d terrains. Computers & Electrical Engineering **39**(6), 1667–1683 (2013)
25. Mikhaylov, K., Petäjäjärvi, J., Haenninen, T.: Analysis of capacity and scalability of the lora low power wide area network technology. In: European Wireless 2016; 22th European Wireless Conference; Proceedings of, pp. 1–6. VDE VERLAG GmbH (2016)
26. Misra, P.: Build a Scalable Platform for High-Performance IoT Applications . Tech. rep., TCS Experience certainty (2016)
27. Nef, M.A., Perlepes, L., Karagiorgou, S., Stamoulis, G.I., Kikiras, P.K.: Enabling QoS in the internet of things. In: Proc. of the 5th Int. Conf. on Commun., Theory, Reliability, and Quality of Service (CTRQ 2012), pp. 33–38 (2012)
28. Neiva, F.W., David, J.M.N., Braga, R., Campos, F.: Towards pragmatic interoperability to support collaboration: A systematic review and mapping of the literature. Information and Software Technology **72**, 137–150 (2016)
29. Saint-Andre, P.: Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 3920, RFC Editor (2004). URL `https://www.ietf.org/rfc/rfc3920.txt`
30. Sarkar, S., Kundu, A.: An Indexed Approach for Multiple Data Storage in Cloud. In: Information Systems Design and Intelligent Applications, pp. 639–646. Springer (2016)
31. Schoop, M., Moor, A.d., Dietz, J.L.: The Pragmatic Web: A Manifesto. Commun. ACM **49**(5), 75–76 (2006)
32. Shelby, Z., Bormann, C.: 6LoWPAN: The Wireless Embedded Internet, vol. 43. John Wiley & Sons (2011)

33. Singh, M., Rajan, M.A., Shivraj, V.L., Balamuralidhar, P.: Secure MQTT for Internet of Things (IoT). In: Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on, pp. 746–751 (2015)
34. Sun, W., Choi, M., Choi, S.: Ieee 802.11 ah: A long range 802.11 wlan at sub 1 ghz. Journal of ICT Standardization **1**(1), 83–108 (2013)
35. Ungurean, I., Gaitan, N.C.: Data distribution service for real-time systems-a solution for the internet of things environments. Annals of the University Dunarea de Jos of Galati: Fascicle II, Mathematics, Physics, Theoretical Mechanics **38**(1), 72–76 (2015)
36. Vasco Lopes, N., Pinto, F., Furtado, P., Silva, J.: IoT architecture proposal for disabled people. In: IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 152–158 (2014). DOI 10.1109/WiMOB.2014.6962164
37. Van der Veer, H., Wiles, A.: Achieving technical interoperability. European Telecommunications Standards Institute **3**, 1–30 (2008)
38. Vinoski, S.: Advanced message queuing protocol. IEEE Internet Computing **10**(6), 87–89 (2006)
39. Wang, C., Daneshmand, M., Dohler, M., Mao, X., Hu, R., Wang, H.: Guest Editorial - Special Issue on Internet of Things (IoT): Architecture, Protocols and Services. Sensors Journal, IEEE **13**(10), 3505–3510 (2013)
40. Whitmore, A., Agarwal, A., Da Xu, L.: The internet of things—a survey of topics and trends. Information Systems Frontiers **17**(2), 261–274 (2015)
41. Winter, T.: Rpl: Ipv6 routing protocol for low-power and lossy networks. RFC 7252 (2012)
42. Xu, K., Qu, Y., Yang, K.: A tutorial on the internet of things: from a heterogeneous network integration perspective. IEEE Network **30**(2), 102–108 (2016)
43. Yang, Z., Ping, S., Sun, H., Aghvami, H.: CRB-RPL: A Receiver-based Routing Protocol for Communications in Cognitive Radio Enabled Smart Grid. IEEE Transactions on Vehicular Technology **65**, 1–10 (2016)
44. Z. Shelby, K.H., Bormann, C.: The Constrained Application Protocol (CoAP). RFC 7252, RFC Editor (2014). URL `https://tools.ietf.org/html/rfc7252.txt`
45. Zaloker, Joseph: ANT/ANT+. Tech. rep., Arrow M2M representative (2014)