Received: 7 March 2018 | Revised: 3 June 2018 | Accepted: 18 July 2018
DOI: 10.1002/cpe.4946

WILEY

SPECIAL ISSUE PAPER

An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols

B.B. Gupta | **Megha Quamara**

National Institute of Technology Kurukshetra, Kurukshetra, India

Correspondence
B.B. Gupta, National Institute of Technology Kurukshetra, Kurukshetra, India.
Email: gupta.brij@gmail.com

Funding information
SERB, DST, Government of India, Grant/Award Number: SB/FTP/ETA-131/2014

Summary

Understanding of any computing environment requires familiarity with its underlying technologies. Internet of Things (IoT), being a new era of computing in the digital world, aims for the development of large number of smart devices that would support a variety of applications and services. These devices are resource-constrained, and the services they would provide are going to impose specific requirements, among which security is the most prominent one. Therefore, in order to comprehend and conform these requirements, there is a need to illuminate the underlying architecture of IoT and its associated elements. This comprehensive survey focuses on the security architecture of IoT and provides a detailed taxonomy of major challenges associated with the field and the key technologies, including Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN), that are enabling factors in the development of IoT. The paper also discusses some of the protocols suitable for IoT infrastructure and open source tools and platforms for its development. Finally, a brief outline of major open issues, along with their potential solutions and future research directions, is given.

KEYWORDS

authentication, Internet of Things (IoT), protocols, RFID, security, WSN

1 | INTRODUCTION

Internet has revolutionized the world to an extent that we can barely imagine our lives without it. The traditional Internet was spread across the two dimensions of time and space, which provided time unbounded wireless connectivity to the electronic devices across the globe. However, the immense growth in the field has lead to a scenario in which any object in our surroundings can be made digital, along with support of wireless accessibility. This digital transformation of things has been termed as Internet of Things (IoT). IoT aims at establishing a ubiquitous computing environment, in which everyday things would support interoperability in order to achieve a common goal. It can be viewed as an interlinking of physical world with the Internet. With the rapid development in the field, a variety of applications are coming up to serve in our everyday lives. These applications are not just restricted to surfing the web to collect the information, chatting with someone sitting on the other end of the network, or to any specific business and context. However, with these applications, we can also control our physical environment. For example, one can remotely control the parameters of a temperature sensor deployed in a dense forest or can turn the air conditioner on or off to adjust the room temperature regardless of the physical presence in that room. Figure 1 shows the major elements of the IoT environment.

With IoT, everyday things are supposed to get a digital identity with which they can be identified and can communicate with each other in order to exchange information and to access numerous services. The idea of digital identification of a large number of devices leads to the development of new identification technology – Radio Frequency Identification (RFID). However, these devices are not full fledge resource equipped, which inspired the concept of resource-constrained Wireless Sensor Networks (WSNs). Cloud Computing, an Internet-based computing practice, has provided a virtual platform for the integration of processing and storage devices, numerous business services, and development and research tools. Users can get application accessibility on demand regardless of their physical location. Fourth-Generation–Long-Term Evolution (4G-LTE) is providing high-speed Internet connectivity to the end users, thereby showing a transition toward leading-edge next-generation technologies. With the advent of these technologies, conventional protocols and standards are getting replaced by some novel ones such as IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN), ZigBee, WirelessHART, Message Queuing Telemetry Transport (MQTT), and so on. IoT applications are spanning

FIGURE 1 The four major elements of IoT environment

various industrial domains extending from smart homes to smart healthcare, transportation, agriculture, retail, and wearable, thereby simplifying and enabling control over the routine work life and personal activities.

While these technologies, protocols, and standards are driving force for the growth of IoT, they are also introducing new challenges in the field related to the integration with conventional framework of the Internet and network scaling, along with IoT specific challenges, such as device heterogeneity, ambiguity in standardization of its framework, etc. Attack scenarios are also proliferating due to the increase in number of edge devices that serve as entry points to the network. Zero day attacks, Ransomware, and identity exposure are becoming common real-time threats with the growing cyber ecosystem. Hence, establishing security in IoT is not just about making a single machine secure but securing devices in bulk that are expected to work in collaboration with each other.

In literature, the domain of IoT has been widely studied in terms of different aspects. Yan et al[1] provide a detailed study of trust management in IoT with a research model to achieve the same. Li et al[2] present a survey on IoT with an emphasis on its service-oriented nature. Granjal et al[3] present a survey on the communication protocol stack in IoT along with some open research issues associated with it. Ngu et al[4] present a survey on the issues and the enabling technologies associated with the IoT middleware. Adat and Gupta[5] provide a survey of security issues and defence mechanisms in IoT. However, none of them addresses the issues associated with other different aspects at fine-grained level, including the system entities and IoT-specific features that are required to be illuminated. In order to facilitate the progress of IoT, it is required to have an understanding of the IoT environment and to get acquainted with the development related to the underlying architecture, algorithms, tools, and protocols. It is required to figure out the enabling factors for its development, the associated risk factors and resulting challenges, the security issues that are yet to be addressed, and security mechanisms that can be adopted to overcome the same. In this paper, we study all these aspects related to IoT environment in detail. The contribution of this survey paper with respect to other surveys is summarized as follows:

- A detailed discussion on architecture of IoT along with the associated entities.
- A taxonomy of issues associated with IoT paradigm on the basis of different aspects including architecture, entities, technologies, and features.
- A deeper summary of the Internet Engineering Task Force (IETF) protocols associated with IoT networks, along with some challenges and existing solutions.
- A taxonomy of open source tools and datasets available for research and development in IoT.

The remainder of the paper is organized as follows. Section 2 describes the historical background of IoT, statistics, and growth predictions related to the field, along with motivation behind establishment of secure ecosystem for IoT. In Section 3, we introduce the layered security architecture of IoT and key underlying technologies at each layer. Section 4 provides a taxonomy and brief analysis for the key challenges in the growth and development of IoT. Section 5 covers the technology specific challenges and existing solutions for RFID and WSN. In Section 6, some of the protocols, particularly given by IETF and a brief comparison between ZigBee and WirelessHART is given. Section 7 describes some of the open source tools and platforms, along with datasets for research and development in IoT. Section 8 covers some of the major open challenges, ongoing research and development activities, and future research directions. Finally, Section 9 concludes the paper.

2 | HISTORICAL BACKGROUND, STATISTICS AND MOTIVATION

The emergence of IoT is one of the remarkable phenomenon in the history of digital computing. The term IoT was coined in the year 1999 by Kevin Ashton who is one of the co-founders of Auto-ID Center at Massachusetts Institute of Technology (MIT), United States.[6] He described it as a system of interconnection between physical world and the Internet through the use of RFID and pervasive sensor devices that observe and identify the real world. However, the concept of interconnectivity among smart devices came into picture in early 1980s when a modified coke machine at Carnegie Mellon University, United States, was connected to the Internet to check and report the inventory for the availability of the drinks.[7] In 1991, present-day vision of IoT was given by Mark Weiser's in his paper on pervasive computing – The Computer of the 21st Century.[8,9] Table 1 shows the major events associated with the growth of IoT from the year 1999 to 2017.

IoT is offering a pool of opportunities to all the stakeholders, including hardware manufacturers, application developers, Internet Service Providers (ISPs), researchers, and industrialists. These opportunities are associated with the evolution of traditional Internet, which provided services and applications for information transfer, communication, and analysis in a pervasive computing environment in which physical objects can be controlled and environment can be sensed. In 2005, ITU proposed that IoT will establish intelligent connectivity and sensing capabilities among the

TABLE 1 Evolution of IoT during 1999-2017

Year	Events
1999	The term "Internet of Things" was coined; First M2M protocol MQTT* was developed.
2000	LG introduced the world's first Internet-connected refrigerator.
2001	National Science Foundation, USA, established Industry-University Cooperative Research Center (IUCRC) to use IoT based predictive analytics technology.
2002	Sony and Philips announced to develop Near Field Communication Technology (NFCT) in co-operation.
2003	IoT was mentioned in one of the main-stream publications "The Guardian."
2004	Wi-Fi hotspots were offered by AT&T and other carriers.
2005	International Telecommunication Unit (ITU) published its first report on IoT.
2006	Nokia introduced Bluetooth Smart Technology under the name "Wibree."
2007	European Union based organization European Research Cluster on IoT (IERC) was founded.
2008	More Internet-connected devices than people.
2009	The first browser-based cloud application Google Apps was launched.
2010	The first online Tide Monitoring System was developed by IoT company ioBridge.
2011	Creation of the IoT Global Standards Initiative (GSI).
2012	World IPv6 launch.
2013	Internet.org ** was launched.
2014	IoT Incubation Council was launched.
2015	Internet of Things Security Foundation (IoTSF) was launched.
2016	"Mirai" malware was used to conduct DDoS attack powered by IoT devices.
2017	IoT One*** created an IoT Terms Database.

*MQTT is a lightweight, publish-subscribe–based messaging protocol developed by Dr. Andy Stanford-Clark (IBM) and Arlen Nipper (Cirrus Link) for resource-constrained devices, and low-bandwidth, delay-prone and unreliable networks.[10]
** Internet.org is a partnership between social networking services company Facebook and six other companies, including Samsung, Nokia, Ericsson, MediaTek, Qualcomm, and Opera Software, which aims to provide economical access of preferred Internet services to less developed nations by improving efficiency and supporting the development of new business models around the provision of Internet access.[11]
*** IoT One is a trusted source for structured information about Industrial Internet of Things (IIoT).[12]

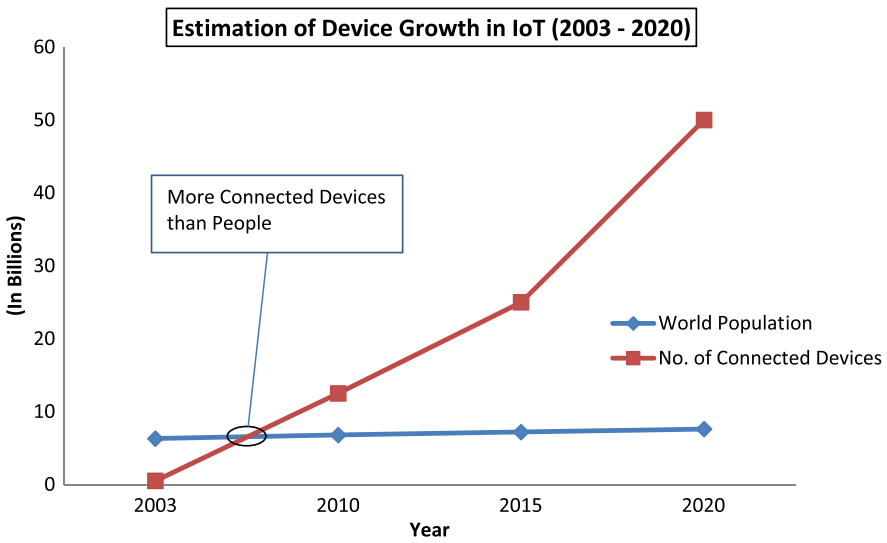

FIGURE 2 Estimation of comparative growth in world population and number of Internet-connected devices by the year 2020 (according to Cisco IBSG, April 2011)

real-world objects.[13] According to results estimated by Cisco Internet Business Solutions Group (IBSG) as shown in Figure 2, there will be around 50 Billion devices connected to the Internet by the year 2020.[14] From this plot, it can be observed that the number of Internet-connected devices exceeded the world population in 2008. Figure 3 shows the estimated growth in the number of Internet-connected devices per user between 2003 and 2020. In 2011, traffic of a cellular network in United States, when monitored, showed an increase of 250% in Machine-to-Machine (M2M) traffic volume. It is expected that by the year 2022, 45% of the whole Internet traffic would be M2M based.[15] Economic efficiency of industries is highly dependent on IoT based intelligent services. Wikibon predicts that the yield from industrial Internet will be around $1200 billion in 2020 with Return on Investment (ROI) growing to 149% compared to 13% in the year 2012.[16] International data Corporation (IDC) Health Insights anticipates that

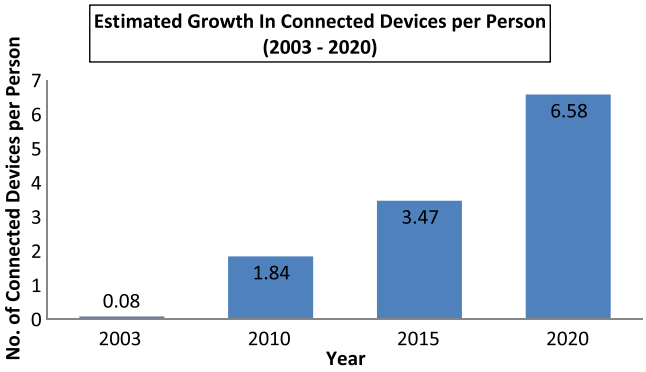

FIGURE 3 Estimation of growth in number of Internet-connected devices per person by the year 2020 (according to Cisco IBSG, April 2011)

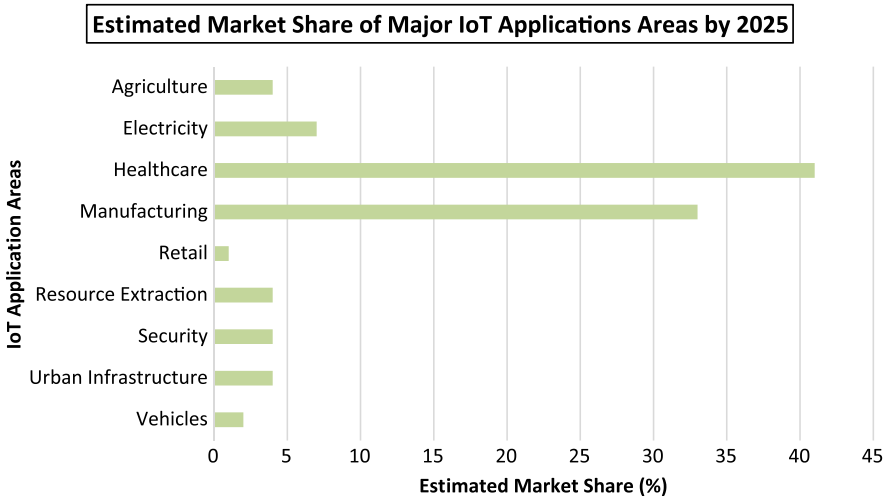

FIGURE 4 Estimated market share of major IoT applications areas by 2025 (according to McKinsey Global Institute, 2013)

by 2020, 80% of the consumer service interactions will involve IoT to improve quality, value and timeliness of care which has been termed as smart healthcare.[17] Low power consuming sensor networks and mobile devices along with interactive applications and services brought the idea of smart cities. Efficient resource management and smart transportation management are some of the trending application areas of IoT.

Figure 4 shows the estimated market share of some of the key application areas of IoT by the year 2025.[2] According to the results estimated, applications having major impact would be healthcare and manufacturing. Advancements in digital electronics has resulted in miniaturization of devices that have the capability to monitor and sense the physical environment, to perform complex computations over the collected data, and to wirelessly communicate the information to other nodes of the network without human interaction. All these statistics reflect the rapid advancement in the Internet and device technology and a fast-pace growth of IoT in the near future. Such a tremendous increase makes it important to outline and resolve the existing issues in IoT and to anticipate the future challenges in order to promote this emerging domain. There is a demand for researchers, people from government organizations, private firms, and from other segments to work collaboratively in order to frame policies and standards for this domain.

3 | ARCHITECTURE OF IoT

Realization of IoT is possible through the integration of numerous enabling technologies including WSN, RFID, M2M, and Low Power Personal Area Networks (PAN). To understand the key role, they are likely to be playing in IoT, a number of frameworks for IoT have been proposed. Many well-known International organizations and working groups including ITU,[18] Institute of Electrical and Electronics Engineers (IEEE),[19] Cisco,[14] and European Telecommunications Standards Institute (ETSI)[20] have presented IoT frameworks on the basis of application requirements, network topology, protocols, business and service models, and so on. However, none of them have been standardized up to till date. Since IoT will be applied to diverse applications areas such as health care, smart transportation systems, and industrial management that are crucial for national economy with different industry standards and specifications, hence security issues require primary attention in order to develop reliable systems and applications. Moreover, for the development of large-scale heterogeneous networks of constrained objects engaged in real-time interactions, architecture of IoT should be resilient enough to address various factors like Quality of Service (QoS), modularity, reliability, semantic interoperability,

<table>
<tr><th>Layers</th><th>Sub-layers</th><th>Key Features</th><th>Key Technologies</th></tr>
<tr><td rowspan="2">Application Layer</td><td>IoT Applications</td><td rowspan="2">Handheld Devices, Terminals and User Interface</td><td rowspan="2">Cloud Computing, Middleware, M2M, Service Support Platform</td></tr>
<tr><td>Application Support Layer</td></tr>
<tr><td rowspan="3">Transmission Layer</td><td>Local & Wide Area Network</td><td rowspan="3">Connectivity Establishment and Information Transmission</td><td rowspan="3">Internet, GPRS, Wi-Fi, Ad hoc Network</td></tr>
<tr><td>Core Network</td></tr>
<tr><td>Access Network</td></tr>
<tr><td rowspan="2">Perception Layer</td><td>Perception Network</td><td rowspan="2">Sensing, Identification, Actuation and Communication Technologies</td><td rowspan="2">RFID, WSN, GPS, Bluetooth</td></tr>
<tr><td>Perception Nodes</td></tr>
<tr><td>Network Management</td><td colspan="2">Physical and Information Security Management</td><td>Trust Management</td></tr>
</table>

FIGURE 5 IoT architecture

privacy management, support for new device types and services, etc. These factors promote the design and development of systems that provide functionality in a reliable and efficient manner.

In this paper, we have focused on the security architecture proposed by ITU - Telecommunication Standardization Sector Y.2002 (Figure 5).[18,21] According to this architecture, IoT can be divided into 3 layers – Perception Layer, Transmission Layer, and Application Layer. Depending on the functionality, these layers have been divided into sub-layers. These are discussed in the following sub-sections.

3.1 | Perception layer

Perception Layer[22,23] can also be known as "Device Layer," "Sensory layer," or "Recognition Layer." It is considered as the bottom-most layer of the IoT architecture. It includes technologies used for sensing (collecting the data from the surroundings and sending it to databases, data warehouses, or Cloud), identification (identifying objects on the basis of unique identity assigned to them), actuation (performing a mechanical action based on the sensed data), and communication (establishing connectivity among heterogeneous smart devices) with minimum human interaction. It is characterized by capturing the information from the real world and representing it in the digital format. Depending on the functionality it serves, this layer can be divided into two sub-layers –Perception Nodes (or Sensory Nodes) and Perception Network.

3.1.1 | Perception nodes

These include the physical devices or objects such as sensors, actuators, controllers, etc. These devices can form an Ad hoc network, a mesh network, or a multi-hop environment in order to increase scalability and faster deployment.[2] Depending upon the underlying technology, these physical devices can be RFID readers, Quick Response (QR) code or Barcode readers, Global Positioning System (GPS) devices, Bluetooth devices, different kinds of sensors (light, humidity, temperature), etc, whose purpose is to collect information from the surroundings, object identification, data control, and object control. Depending upon the nature of devices used, information collected can be related to object properties such as its location, motion, proximity, temperature, humidity, pollutant level, and other environmental conditions. RFID readers can be used to identify the objects on the basis of information collected from the tags associated with them. Object control involves controlling the operational parameters of the devices in order to manipulate the functionality as desired. For example, a sensor device can be programmed to stay in doze mode unless any activity or event is detected in order to save energy and it comes into active mode in order to capture the relevant information. Microchips are embedded in the body of the objects that cannot be perceived directly. These chips are programmed to sense the environment in an intelligent manner. Thus, nanotechnology comes into picture, which ensures that the design of the chip should be small enough to get placed within the body of the objects.[24]

3.1.2 | Perception network

It is responsible for communicating with the Transmission network. It transmits the data collected by the perception nodes in a secure manner to the gateways for further transmission and sends control signals to the controller devices through wired or wireless communication medium.

3.2 | Transmission layer

The Transmission Layer can also be called as "Transportation Layer," or "Network Layer." It is interposed between the perception and the application layer. It can be viewed as an integration of a variety of heterogeneous legacy networks, technologies, and protocols. Its purpose is to transmit the data

gathered by the perception nodes to the information processing unit (or high level decision-making units) using wired or wireless communication channels for analysis, data mining, data aggregation, and data encoding.[1] It is also responsible for providing functionality for network management. Depending upon the functionality it serves, it can be divided into three sub layers – Access Network, Core Network, and Local and Wide Area Network.

3.2.1 | The access network

Access Network provides a pervasive access environment for the perception layer. It is a type of telecommunication network which serves as a bridge between the subscriber and the service providers. It establishes communication and infrastructural capabilities like mobile communication, satellite communication and wireless communication for the end users. Access networks that IoT can implement are Ad hoc network, GPRS network, 2G and 3G (eg, UMTS - Universal Mobile Telecommunications Service) network, Wi-Fi network, ZigBee, Low Energy Bluetooth, etc. 4G-LTE and 5G are advanced telecommunication standards that would provide high-speed Internet connectivity to mobile devices. Depending on the presence or absence of a central station (or base station), access network can be centralized or non-centralized.[25] Wi-Fi is an example of centralized network, while Ad hoc network is an example of non-centralized network.

3.2.2 | The core network

The core network is the Internet which provides the basic framework to the IoT. It is responsible for the transmission of data to the end users who are connected through the access network. It is the central part of any telecommunication network and serves as a backbone for the exchange of information and services. It establishes communication among constrained devices for resource sharing. Internet can be utilized as public or private network, business, or government network and has local as well as wide area scope.[26] It provides capability of observing and controlling the physical objects remotely.

3.2.3 | Local and wide area network

Local Area Network (LAN) is an interconnection between devices within a relatively smaller region. Devices in a LAN can directly communicate among themselves and can communicate with remote devices using gateways. It can be viewed as an integration of access and core network, where former provides the infrastructure and latter provides the access services. In the similar fashion, Wide Area Networks (WANs) are regarded as distribution of devices over larger geographical areas. Low Power Wide Area Networks (LPWANs) are gaining attention because they support connectivity among low power devices.[27]

3.3 | Application layer

This is the topmost layer of the IoT architecture which is visible to the end user. The purpose of application layer is to manage and provide the applications globally on the basis of information collected by the perception layer which in turn is processed by the information processing unit. It provides access of personalized services to the end users over the network according to their requirements through the use of various handheld devices and terminal equipment.[22] It can be divided into two sub layers – Application Support Layer and IoT Applications.

3.3.1 | The application support layer

It is present just above the Transmission layer. It provides support to variety of enterprise services and is responsible for performing intelligent computations and processing over data. It performs data recognition and filtration in order to categorize it as valid, invalid, malicious, spam data, and so on. It utilizes Service Oriented Architecture (SOA) to facilitate QoS, directory service, etc. According to different services, this layer can be organized in different ways.[21] It exploits the functionalities of middleware, which is responsible for intelligent computations and consists of servers for deployment of software on different operating systems and platforms, Cloud Computing which can be viewed as a network of remote servers for storing and processing of data, M2M application model which provides direct connectivity between devices either through wired or wireless links, and the Service Support Platform which provides support services and user interface for the applications. Support services may include general support services, such as processing of data, data storage, and application-specific support services.[18] Advances in Cellular Wide Area M2M connectivity solutions and Low Power Wide Area M2M technologies (LoRa, Sigfox) reflect the increasing importance of M2M in IoT.[28]

3.3.2 | IoT applications

IoT applications can be divided into three categories on the basis of their functionalities – information collection, analytics, and real-time decision-making applications.[4] Information collective applications are responsible for collecting the data from the perception nodes and its local storage, analytics deals with offline pre-processing of collected data to create a generic model for the evaluation of data that is to be collected in future, and real-time decision-making applications are involved in taking the appropriate actions according to the analysed sensed data. IoT has a wide application domain as shown in Figure 6. These applications can be seen as realization of industry demands. These include consumer-oriented

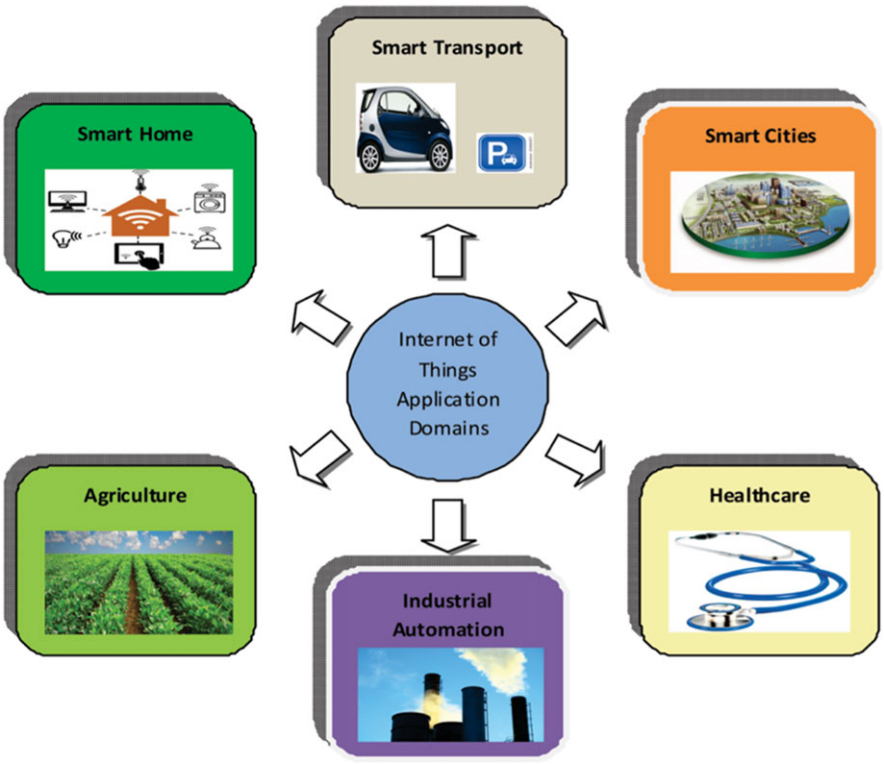

FIGURE 6 IoT application domains

applications like wearable devices, smart homes, and smart healthcare; commercial applications like logistics and retail; industrial applications like resource and energy management, intelligent transportation, and manufacturing; and applications specific to public sector like smart cities, safety and surveillance, etc, that aim at improving the quality of human lives. IoT applications and services are directly accessible to users through the use of various handheld devices like mobile phones, computers, Personal Digital Assistants (PDAs), etc.

3.4 | Backbone features for IoT as a whole

Network Management deals with the topological aspects and efficient resource management. EXtensible Messaging and Presence Protocol (XMPP) based infrastructure,[29] Software Defined Networking (SDN),[30] and Game Theoretic Mechanisms[31] are some of the recent approaches towards efficient network and resource management in IoT environment. Physical and Information Security Management deals with protecting the interconnected physical devices as well as well as ensures secure information storage and transmission among the devices. Increasing number of smart devices raise the requirement of transparent security management techniques that deal with the security of software, web interface, network, and mobile services in order to ensure information confidentiality, integrity, and user privacy. Trust Management plays a key role in the development of IoT environment by providing reliable services to the end users with enhanced user privacy. It helps in reducing the uncertainty and risks associated with the IoT applications and increases the user's acceptance for these applications. Trust in IoT is associated with data perception, processing, transmission, communication, users, and applications. In literature, various trust management schemes for IoT environment from the perspective of SOA,[32] RFID, and WSN[33] have been proposed.

4 | TAXONOMY OF CHALLENGES IN IoT

IoT is a novel research paradigm having a great potential that can change the shape of the conventional use of Internet. However, along with its capabilities, there comes all kinds of challenges at different layers of its architecture and of different aspects that are needed to be addressed. Figure 7 outlines four main categories of challenges in IoT – architecture based, entity based, technology based, and feature based. The proposed taxonomy has been designed by systematically examining the security architecture of IoT in a heterogeneous environment of resource-constrained devices.

Architecture-based challenges cover layer specific issues as well as issues related to the integration of layers into a unified framework. Entity-based challenges focus on challenges associated with the large scale implementation of three fundamental entities of any computing system – hardware, software and data. Technology-based challenges cover challenges associated with underlying supporting technologies of IoT

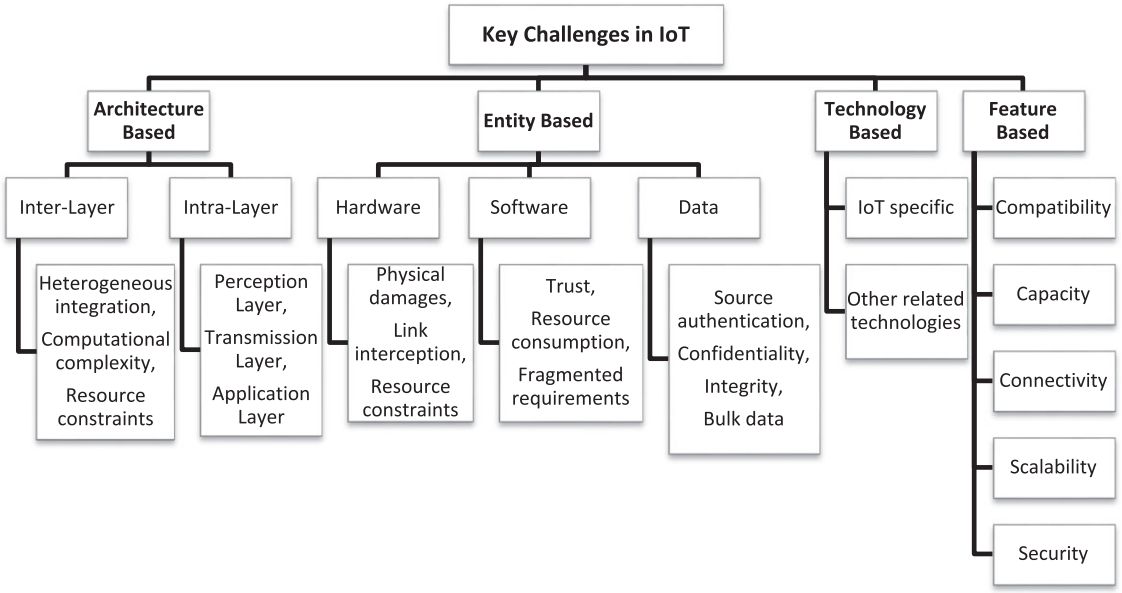

FIGURE 7 Key challenges in IoT

as well with IoT itself. Lastly, feature-based challenges cover challenges associated with compatibility, connectivity, security, and so on. Following subsections give a brief analysis and summary of the same.

4.1 | Architectural challenges

4.1.1 | Inter-layer challenges

The layers defined in the architecture are accompanied with a great deal of heterogeneity which gives rise to cross-layer heterogeneous integration issues.[21] End users can access the data collected by the perception nodes from the environment through the user applications which in-turn passes through transmission layer. The data can be collected in different ways, in different formats, using different protocols and for different purposes. Hence, data standardization at each layer and mapping on per-layer basis is required. If right integration technology is not ensured, it will lead to the destruction of data or data will be corrupted. Moreover, each layer requires different mechanisms to ensure the security, privacy, and validity of the information. Hence, computational complexity arises due to the different mechanisms adopted at each layer. Cross-layer optimization thus becomes relevant, especially when a large number of heterogeneous devices are getting connected through the Internet. Devices that are deployed to accomplish the functionalities at each layer have different resource requirements. For example, there may be resource-constrained devices such as sensors that record data from the surroundings like temperature readings which is of few kilobytes, while there may be high end servers that aggregate the readings from numerous such temperature sensors and generate bulk data after processing. Hence, in order to ensure efficient collaborative working, at the same time fulfilling the varying resource requirements is difficult.

4.1.2 | Intra-layer challenges

Perception nodes are resource-constrained in terms of storage, processing power, energy etc. Hence, integrating the conventional security mechanisms with their data capturing capability is challenging. They are supposed to be deployed in diverse environmental conditions and are susceptible to physical damages. For instance, sensors to monitor growth of plants may be deployed beneath the surface of earth, or sensors to monitor the tidal activities are immersed in sea water. Moreover, they are vulnerable to attacks like Denial of Service (DoS) and other malicious attempts that can manipulate their operational parameters. Therefore, to ensure that no malicious activity or physical event can disturb their normal working is difficult. Ensuring node authentication and data integrity are other key issues. The device once compromised can produce false results that can affect the functionality of the entire network. Malicious nodes can also be introduced in the network that can access the information for which they are not authorized.

Transmission layer which is mainly Internet is going to be accessed by a large number of devices. In this scenario, network congestion and unique identification of devices add up to existing challenges. This layer is also susceptible to attacks like Distributed Denial of Service (DDoS), phishing, malware intrusion, access attacks, information disclosure, etc. As it is made up of heterogeneous networks, security issues related to heterogeneous fusion may also arise.

Since application layer deals with numerous business-related or individual-specific applications, it is accompanied with general and security issues of all these applications such as service interruption, information disclosure, threat to location, and query privacy. An instance of service interruption could be seen when multiple large DDoS attacks were conducted on October 21st, 2016 by Mirai malware installed on a large number of IoT devices

TABLE 2 Intra-layer technology specific-security challenges in IoT

Layer	Technology (Components)	Security Challenges
Perception Layer	RFID (Tags, Readers, Antenna)	Device tracking, DoS, Repudiation, Spoofing, Eavesdropping, Counterfeiting, Data newness, Unauthorized accessibility, Self-organization, Time management, Secure localization, Tractability, Robustness, Survivability[21]
	WSN (Wireless sensor devices, Central gateway)	DoS, Resource exhaustion, Unfairness, Sybil attack, Jamming, Tampering, Collisions, Node subversion, Node outage, Passive information gathering, False node, Message corruption[35]
	GPS (Ground control stations, Satellites, Receivers)	DoS, Black hole attacks, Eavesdropping, Spamming, Broadcast tempering, Loss of event traceability[36]
	Bluetooth (Antenna, Hardware, Software, Protocol stack, Application)	Eavesdropping, DoS, Bluesnarfing, Bluejacking, Bluebugging, Car whisperer[37]
	ZigBee (Radio, Microcontroller, Protocol)	Eavesdropping, Packet manipulation, Hacking, Key exchange, KillerBee, Scapy[38,39]
Transmission Layer	Wired (Cables, Network adapters, Routers)	Data manipulation, Extortion hack, Equipment hijacking, Malicious attacks[40]
	Wireless (Radio communication, Transmitters, Receivers)	Misconfiguration, Hacking, signal loss, DDoS, War dialing, Protocol tunneling, MITM, Phishing, Routing Information identification[41]
Application Layer	Smart Grids (smart meters, smart appliances, Energy Management System (EMS), Electronic Power Conditioning and Distribution System)	Data stealth from utility servers, Functionality manipulation, DoS, Falsifying energy consumption data, Replay attacks, Physical meter tampering, Mistrust between traditional power devices, Compromised device endpoints, Malicious attacks[42,43]
	Smart Healthcare (Smart health cards, Wearable devices)	Theft and loss, Insider misuse, Unintentional actions, Hacking, Non-auditability, Information disclosure, Sybil attack[44,45]
	Intelligent Transportation (Transit Management System (TMS), Electronic Toll Payment System, Traffic signal control system, Public transportation, Traveller information services)	DoS, Location disclosure, Manipulation of sensors, Unauthorized access to monitoring equipment, Customer privacy, Broadcast of forged traffic information, Breakdown of key operating components of TMS[21,39]
	Smart Home (Air conditioning system, Lightening system, Automated appliances, Security components)	Eavesdropping of Personal information (Email, Internet surfing, Phone conversations), Traffic analysis (Frequency of messages, Location of home user), Masquerade attacks, Replay attacks, DoS, Session stealing attacks, Malicious codes and scripts[46]

that attacked the DNS services of DNS service provider Dyn and caused service interruptions of various high-profile websites, such as Twitter, GitHub, Airbnb, and many others.[34] Smart devices supporting access to a variety of applications have limited battery power and storage capacity. Thus, they have limited computation capabilities.

Table 2 summarizes security challenges associated with technologies at each layer of IoT architecture.

4.2 | Entity-based challenges

4.2.1 | Hardware

It is necessary to protect the hardware devices, including mass data storage devices, and servers over which software are deployed and applications are running from physical damages. These physical damages can occur due to natural disasters as well as deliberate malicious attempts by the attackers. Safety of wired communication links is also necessary because they are responsible for carrying data from large number of sensor nodes and they can be intercepted as well. Other IoT devices that require safety are hardware tokens (smart cards) or remotely located devices (Internet appliances) that act as interface between the user and the computer. Above that, integrating functionalities over hardware devices that are resource-constrained is challenging.

4.2.2 | Software

Software may include application software, such as communication or security application programs that serve some specific purpose, or system software, such as operating systems or DBMS that are required for the development and execution of the application software. Since IoT facilitates

the use of large number of heterogeneous devices, degree of trust is relatively low. Any attacker can interfere with the normal working of software which may result in huge crisis. Application software accessible to the users also possesses a high degree of vulnerability. One-size-fits-all model cannot be applied to large scale software development because of diverse nature of devices including sensors and wide range of connectivity solutions. Varying level of complexity exists among software required for tasks including data sensing, processing, handling, security establishment etc. As the size of the software increases, resource consumption and overall cost of the system increases. Developing low-cost and low-power solutions for constrained IoT devices and to develop a software ecosystem that can deal with fragmented requirements requires a new design thinking and right engineering decisions.

4.2.3 | Data

Data is the primary user asset in digital environment, and the purpose of any computing system is to deal with data. Therefore, databases containing data also require protection. Data may belong to an individual, a group, or an organization, and level of content sensitivity also varies according to the usage. For example, a person's health records are more sensitive than the temperature readings of a city. It can be accessed, modified, and destroyed in an unauthorized manner. Due to large number of devices participating in IoT, it would be difficult to authenticate the data and its source. Malicious data can be pushed into the network through the communication channels and can create havoc. Developing lightweight schemes based on encryption, digital signature, hash encoding, etc, for safeguarding the data to ensure confidentiality and integrity in a heterogeneous environment with resource-constrained devices is another big challenge. Moreover, data generated by devices in bulk, termed as Big Data, needs lightweight data handling techniques which is still an open area of research.

4.3 | Technology-based challenges

4.3.1 | Challenges specific to IoT

Central concept of IoT is to connect anything, anytime and anywhere through Internet. Supporting a large number of internet-connected heterogeneous devices will be the main challenge in IoT. Assigning unique identity to countless devices getting connected to the Internet is one of the biggest challenges. Introduction of IPv6 as a basic building block for ensuring scalability of the Internet is one solution for this problem.[47] However, device mobility issues, basic topology variations, node miniaturization are again matter of concern for large-scale deployment of IPv6. Global distribution of services, while at the same time ensuring an effective durability of the technical environment require novel regulatory approaches.

4.3.2 | Challenges due to other related technologies

From the construction of the network until implementation of its functionalities, IoT is highly dependent on other technologies including RFID, WSN, Wi-Fi, Cloud Computing, Mobile Computing, Ad hoc Networking, GPS, etc, Internet being the primary among these. Since Internet provides the basic framework for IoT, challenges associated with it would play a crucial role in the development of IoT. Key challenges of WSN include architecture, secure routing protocols, energy optimization, and QoS. Cloud Computing introduces challenges like efficient resource management, QoS, infrastructure scalability, data isolation, recovery, and reliability. Problems related to other enabling technologies will also come into picture.

4.4 | Feature-based challenges

1. Compatibility – IoT is building a large-scale heterogeneous network which consists of all sort of electronic, electrical, and computing devices communicating with each other through Internet. These devices operate on different protocols, run different algorithms, and accept input data in different formats. Thus, compatibility issues are of great concern.
2. Capacity – IoT devices have limited capacities in terms of memory, processing power, battery power, etc. Embedding selective functionalities over them considering capacity constraints must be done in effective manner.
3. Connectivity – For establishing connectivity among the devices, a variety of wired or wireless network control and communication technologies are in use, such as European Installation Bus (EIB), RS-485, Wi-Fi, Bluetooth, ZigBee, etc. Different communication models like Ad hoc networking, Mobile networking, and WSN have been adopted. However, integration of these technologies and models is a big challenge. Moreover, effective addressing schemes need to be developed to deal with identification of devices in bulk.
4. Scalability – IoT applications require a large number of devices for their implementation which becomes difficult because of their different operating characteristics and varying resource requirements.
5. Security – In IoT environment, we are not concerned about the security of a single layer or security of a single element of the IoT framework, but it is about the security of the entire system. If we think from the perspective of TCP/IP model, the security of the network is required at three levels of communication – node level, gateway level, and application level (Figure 8). At node level, the node integrity, access control, and the communication between end devices accessing the web is required to be made reliable and authenticated. At gateway level, the communication between devices behaving as the entry point to the network should be made secure. At application level, the communication between clouds of

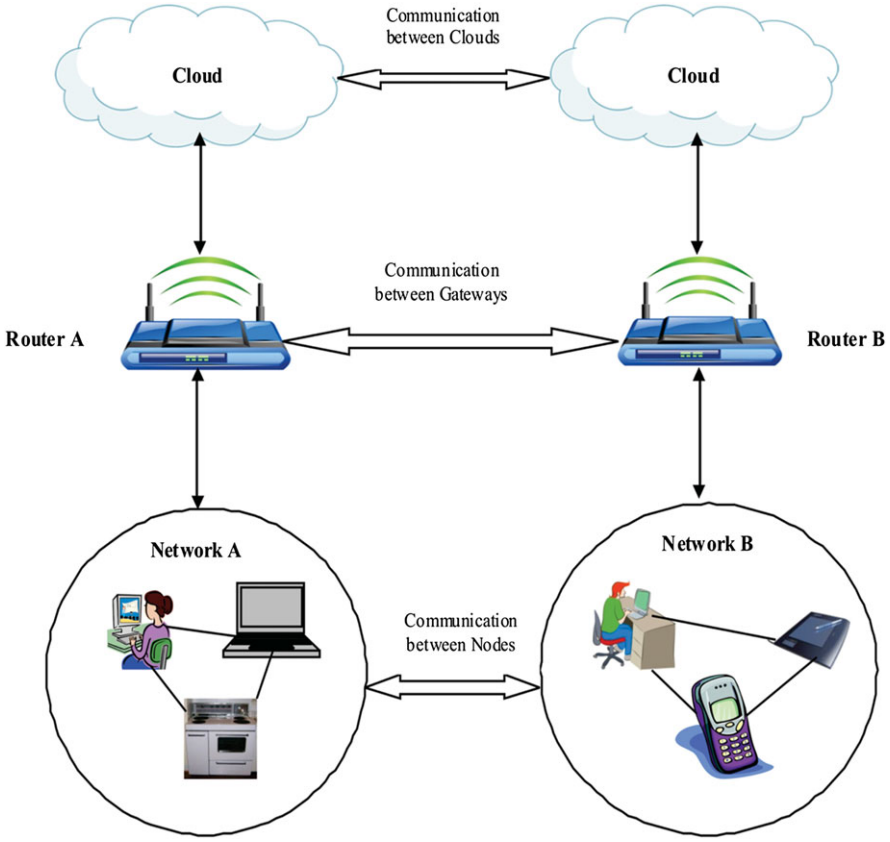

FIGURE 8 3-tier communication in a network

information is required to be made secured. Privacy protection and secure data audits are also required. Hence, layer-specific issues as well as security issues of the system as a whole are needed to be addressed.

5 | ANALYSIS OF SOME TECHNOLOGY BASED ISSUES IN IoT AND EXISTING SOLUTIONS

5.1 | Radio Frequency Identification Technology (RFID)

RFID is a technology which uses radio waves to assist computing devices in automating the process of target object identification, tracking and control electronically, as well as data capturing and recording metadata in a flexible and reliable manner. A typical RFID system is composed of following two components (Figure 9):

1. RFID Tag – A tag is a microchip connected with an antenna which stores information and when attached to an object can act as that object's identifier. The purpose of the coiled antenna is to transmit and receive radio waves for communication between the reader and the tag whenever both are in close proximity of each other. Tags are also known as transponders.[48] They can transmit the signals to other tags as well as respond to reader on receipt of a command. Tags can be active or passive depending on the availability of battery source. Active tags are equipped with battery source and they can communicate with other tags. While passive tags do not have any internal battery source and are powered up by the readers in proximity of tags.
2. RFID Reader – RFID reader uses radio waves to communicate with RFID tag to obtain the relevant data and transmit the collected data to the required application. Hence, it works as both transmitter and receiver (also known as transceiver). An external application is responsible for controlling the reader system via control commands.

5.1.1 | Key issues

RFID is an evolving technology which can be merged with IoT by linking the RFID readers with the IoT devices for real-time identification and monitoring of the objects equipped with RFID tags that are located globally. While RFID is widely used in many applications, such as payment transactions, transportation and toll collection,[49] military and defense, automotive industry, libraries, and so on; it exposes a lot of problems as follows:

1. No Uniform Encoding – To maximize the information exchange, tag information must be encoded uniformly. However, no internationally acceptable uniform encoding standard for RFID tag has been developed up to till date. Since no uniform standard has been created and IoT is aiming

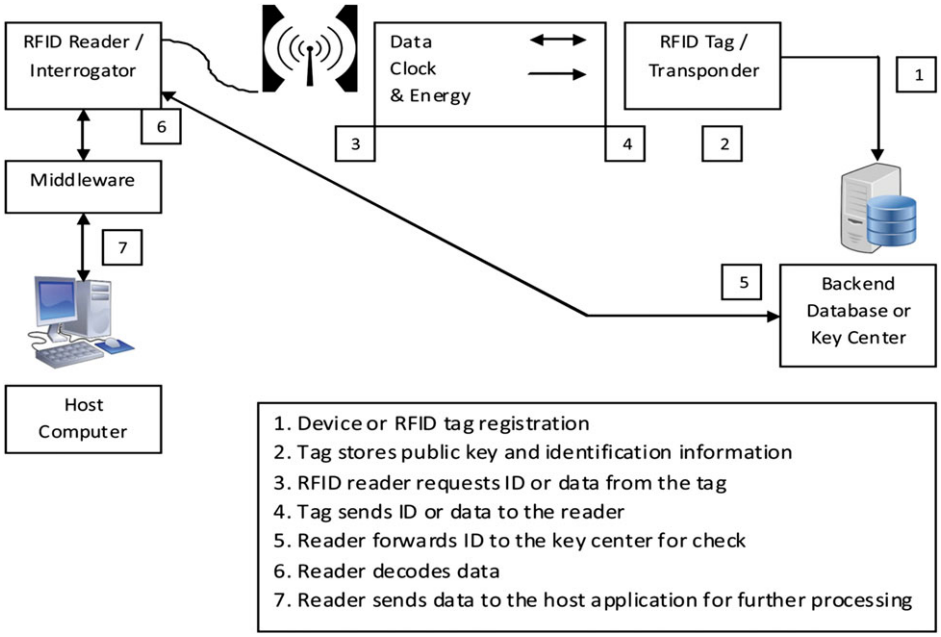

FIGURE 9 A typical RFID system

at providing connectivity between heterogeneous devices, it may cause problems in accessibility of the tag information or errors in the reading process.[21]

2. Conflict Collision Problem – In large-scale applications, simultaneous transmissions occur between readers and tags that are typically operating on the same wireless channel. Hence, communication between tags and readers are intrinsically prone to electromagnetic interference which leads to conflict collision. RFID conflict collision can be divided into two categories – tag's collision and reader's collision. When there are multiple RFID tags in the reader's working scope that are transmitting the information to the reader at the same time, it may cause the reader not able to get the data correctly. This is called tag's collision. IoT requires wide range of RFID sensor coverage and hence deployment of multiple readers that must work in a cooperative manner, but the working scope of reader may overlap. Thus, information may become redundant which will increase the burden on the transmission of the network. This is called reader's collision.
3. Security and Privacy related Problems – Being a resource-constrained and relatively low-cost solution, RFID technology does not have enough security and privacy support. Unprotected RFID tags are prone to passive attacks, such as traffic analysis and eavesdropping as well as active attacks including spoofing, replay attacks, and DoS.[48,50] Tag ID can be used by the hackers to track the location of the tag, thereby breaching the location privacy.[51] Unauthorized RFID readers not having enough access control can also breach the data privacy of the system by accessing the tag information.[48] Figure 10 shows the common security attacks against RFID technology.
4. Trust Management – To ensure node privacy in IoT environment, there is a need to establish trust management in RFID system. Trust management can be established between the readers and the tags, as well as between the readers and the base stations. Digital signature technology is widely used in this domain to avoid counterfeiting of tags and readers. It has been used for data authentication and exchange, as well as for node authentication among different applications for a long time. Standard cryptographic algorithms and protocols that are used for digital sig-

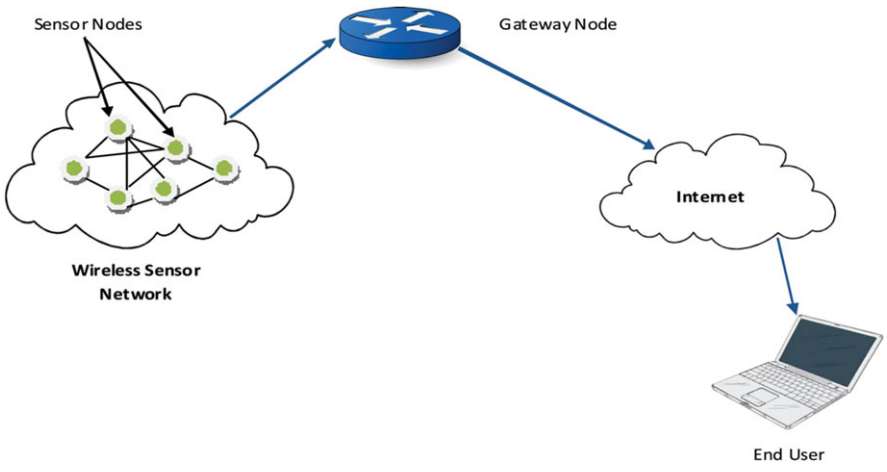

FIGURE 10 Integration of wireless sensor network (WSN) and Internet

nature technology require storage space and computing resources to an extent greater than the available resources of RFID tags. Therefore, RFID authentication algorithm must take into account the issues related to storage and complexity of computing power.

5. Other Challenges – Other issues that are trying to limit the RFID's widespread adoption are complex design, high cost, and interoperability with existing systems. In order to guarantee highly reliable target object identification and control, it is still required to develop tags and readers in a manner so that they can be deployed in large-scale applications. RFID tags are still more expensive than other identification technologies based on bar code, infrared, etc. Another hurdle in wide scale adoption of RFID is its integration with existing systems. It is required to develop effective RFID middleware which can be used to link modern RFID systems with existing back-end infrastructures.[48] Deactivation attacks can render the RFID tag useless, unable to be identified by the reader. Universally acceptable standards and legal framework are still missing for RFID-based systems.

5.1.2 | Existing solutions

Despite these challenges, it is only a matter of time before these issues could be solved. Following are some of the solutions proposed in the literature that can be adopted to resolve these issues.

1. Uniform Coding Standards – Some developed nations have adopted their own standards. The most significant ones are – Universal Identification (UID) standard supported by Japan and the Electronic Product Code (EPC) standard supported by Europe.[21]
2. Avoiding Conflict Collision – Anti-collision mechanisms can be used to prevent conflict collision in RFID systems in order to develop large-scale RFID-based applications. Solutions for reader anti-collision have been categorized as follows – Scope-based solutions and Time-based solutions.[21] In scope based solutions, the working scope of readers is kept separate in order to reduce the conflict zone. In time-based solutions, different time slots are allotted to the readers to send or receive signals to or from the tagged devices. However, both require the presence of central system to determine the working scope and time for readers which will increase the complexity and cost. Many anti-collision protocols have been proposed in the past like slotted ALOHA,[52] advanced dynamic framed slotted ALOHA,[52] Binary splitting scheme,[53] Query tree protocol,[54] etc, but their efficiency is not more than 50%.[48] Thus, demand for better mechanisms arises.
3. Security and Privacy Protection – Many lightweight solutions have been proposed to ensure security and privacy of RFID systems as described in Table 3. Few are based on password based mechanisms including anonymous ID,[21] hash chain,[56] hash locks,[57] etc, while others are based on physical security like Faraday cages,[58] clipped tags, block tags,[49] etc. Some compromising solutions are also there that suggest not to store critical information in RFID tags and to store such information on higher-level service layers. However, none of the solutions provide complete security. Hence, it is an open field of research.
4. Trust Management – To establish trust between RFID nodes, many authentication mechanisms have been proposed. RFID tags can be made physically unique as well as difficult to replicate by using Certificate of Authenticity (CoA).[59] For this, fingerprinting technology can be adopted.[60] RFID security protocols like RWP,[61] AFMAP,[62] and RFID private authentication protocols[63] have been developed. Digital signature technology can also be implemented to ensure data integrity as well as node authentication.[21]

TABLE 3 Comparison of some existing security and privacy protection mechanisms in RFID systems

Security Solution	Examples	Description	Drawbacks
Password Based Mechanisms	Anonymous ID	Technique of storing encrypted identity in the tag	Provides limited privacy
	Hash Chain	Safeguards against information eavesdropping	Computational load is proportional to the number of tags, hence limited scalability
	Hash Locks	Prevents exposure of tag identity	Cannot protect location privacy
Physical Security	Faraday Cages	Isolates tags from electromagnetic waves	Limits the application domains of RFID systems
	Clipped Tags	Tag modification to convert it from long-range tag to proximity tag	Physical destruction of tag can damage the original item
	Block Tags	Prevents unwanted scanning of tags by the readers through simulation of multiple tags simultaneously	Malicious tags can avoid desired tag detection by tag spoofing
Other Solutions	Challenge-Response based Authentication Protocols, eg, Pseudonyms[55]	Used for tag authentication	Can be compromised by a powerful adversary

5.2 | Wireless Sensor Network (WSN) technology

Wireless sensor networks are distributed networks having dynamic topology and consist of spatially distributed autonomous sensor devices that monitor the environment, objects, as well as interactions between environment and objects in a collaborative manner.[64] WSNs are finding their use in wide range of application areas like smart living, industrial automation and production monitoring, healthcare, and many other fields and are expected to be integrated with IoT by forming an independent network, hybrid network, or access point network[65] with the traditional Internet (Figure 10). However, a number of issues are associated with these technologies that are going to impact the development of IoT. Thus, before taking the advantage of this integration, these issues are needed to be tackled. These are discussed in the following sub-section.

5.2.1 | Key issues

1. Security Issues – Security level in WSNs having no Internet connectivity depends on the application sensitivity. Sensor nodes are responsible for ensuring data confidentiality and integrity as well node authentication. The attack scenarios that have been spotted up to till date require physical proximity to the target WSN in order to hinder the normal functionality by physically damaging the sensor nodes or by introducing malicious nodes into the network. However, providing Internet connectivity to WSN nodes in the IoT environment would open up the possibility of massive attacks including zero day attacks, regardless of the physical location. It would become easier for the attackers to introduce malware from anywhere using the Internet. Sensor nodes mapped with gateway's functionalities are unable to reuse the existing security mechanisms directly due to scarcity of resources.[64] Moreover, existing cryptographic techniques based on larger key lengths are not supported by sensor nodes.
2. Cryptographic Algorithms – Diverse application areas of WSNs demand high level of data security which includes preventing unauthorized access and modification of data which can be ensured by data encryption. Data encryption algorithms are divided into two categories – Public key encryption algorithms and Private key encryption algorithms. Public key algorithms offer good scalability, and are suitable for node authentication and for ensuring security of the whole network without the need of complicated key management protocol. However, their high energy consumption and computational complexity makes it difficult to be applied to WSNs having nodes with limited computational power and storage capacity. On the other hand, private key encryption algorithms are widely used in WSNs because of their easy calculations. However, they have the following issues[21] – (1) Digital Signature cannot be applied to ensure authentication. Instead message authentication code is used which increases communication load and requires additional storage space thereby increasing the power consumption, (2) Key exchange protocol is too complex and results in poor scalability of the network, (3) Key confidentiality. Once a node is compromised, it can be a huge security threat for the entire network. To summarize, both of the techniques have their own advantages but none of them can solve the issues of WSNs in the IoT environment completely.
3. Key Management – Key management is one of the key issues yet to be solved for the security of WSNs. It includes secret key generation and distribution, storage, updating and destruction process.[21] Key distribution is the most important issue in key management which involves the distribution of the public key and the secret keys in a secure manner to the legitimate users. The databases maintained for storing keys are vulnerable to attacks. One of the main challenges is to develop a lightweight key distribution scheme for the sensor nodes with limited resources which can be implemented at all levels of IoT layers in order to support diverse protocols, applications, and services.
4. Routing Protocols – Routing mechanisms at network layer play an important role in WSNs. Establishment of secure and efficient routing protocol is required to prevent the network collapse in attack scenarios over the routing protocol. Since sensor nodes have limited power, computational capability as well as storage capacity, conventional routing protocols cannot be employed in IoT environment.
5. Quality of Service (QoS) – Gateway nodes in WSNs act as repeaters and are responsible for translating the protocols under different frequencies.[64] Hence, sensor nodes are also expected to ensure quality of service by optimizing the resource usage of all the heterogeneous devices that are going to be a part of IoT environment. This can be done by exploiting the resource differences and by distributing workload among the devices offering resources accordingly. Consequently, this collaborative working is going to ensure support for security mechanisms. However, existing mechanisms for ensuring QoS are not applicable for IoT scenario, as in real-time environment sudden changes in wireless links can cause reconfiguration of the WSN's topology in a significant way.
6. Configuration Management – Various tasks like self configuration, address management for constructing scalable networks, detection and elimination of faulty nodes to ensure self-healing capabilities would become necessary for the sensor nodes in order to control the configuration of WSNs.[64] However, these features are not common for the participating nodes in the existing Internet. Instead, the user is responsible for installing applications and recovering the system from failures. Hence, for autonomous sensor nodes existing means of configuration management would not work.
7. Trust Management – Nodes in WSNs are resource-constrained and can be easily compromised. Sensor nodes are responsible for collecting information from the surroundings and reporting it to the base station.[21] All these characteristics make WSNs more vulnerable to a number of attacks. Even password based mechanisms and cryptographic algorithms cannot ensure complete security of WSNs as a whole. In WSN environment, sensor nodes work in a cooperative manner, and if a single node gets compromised, it can send false or malicious data to other nodes as well as to the users, thus compromising the security of the whole network. In such scenarios, trust management mechanisms come into picture. However, due to limited resources, trust management system must be able to trade off between limited resources and security of the network.[66]

5.2.2 | Existing solutions

1. Data Security – Some of the symmetric key encryption techniques currently in use are RC4,[67] RC5,[68] and IDEA.[21] In WSNs, symmetric key encryption techniques are relatively easy to use; however, their security strength is not very high and key management is complex. Based on these difficulties, public key encryption techniques have been developed. Some of the key techniques suitable for WSNs are Elliptic Curve Cryptography (ECC) ,[69] Rabin's encryption scheme,[70] etc. However, due to high energy consumption these are difficult to implement in energy-constrained devices. So how to encourage the use of these techniques is an ongoing debate. Shen et al[71] proposed an ECC-based certificate-less protocol for resource-constrained wireless body area networks to protect user's information over insecure communication channels while at the same time ensuring user anonymity. Li et al[72] proposed a malware detection system SIGPID based on machine learning to classify applications as benign and malicious. This model can be adopted to prevent introduction of malware by the attackers using Internet applications.
2. Key Management Schemes – To avoid high energy consumption of devices due to public key based schemes, many symmetric key based schemes have been proposed,[21] such as the random pre-distribution key scheme,[73] centralized key distribution scheme SPINS,[74] q-composite, and a series of other schemes proposed on the basis of random pre-distribution key.[75] However, researchers continue to develop key management schemes based on the advantages of both symmetric and asymmetric key based schemes.
3. Secure Routing Protocols – A number of secure routing protocols have been designed specifically for WSN.[76] Data-centric protocols like SPIN,[77] in which data is requested from a specific set of nodes located at selected regions through negotiation, provide data validity and consistency. However, they lack data authentication. Hierarchical protocols like LEACH[78] focus on improving the scalability and robustness of the network. They perform aggregation of data to avoid false alarms and avoid redundant data flow to the base station. However, they are susceptible to selective forwarding and HELLO flooding attacks. Network Flow and QoS-aware protocols like minimum cost forwarding protocol lay emphasis on reducing the cost of information flow between the nodes. However, they are also susceptible to sink-hole attacks.[79] When it comes to the deployment of these protocols in the IoT environment, a number of novel security challenges are yet to be solved.
4. Trust Management – To understand the importance and implementation of trust management, the researches that have been conducted till date have been classified into following classes – trust measurement mechanism, trust evaluation mechanism, trust relationship formalization, formal derivation of trust, and trust update.[21] Degree of trust depends upon how frequently the sensor nodes are communicating with each other. To ensure the security of the whole network, trust management must be integrated with the security framework of WSNs and IoT. In the work of Yao et al,[80] a distributed trust model aiming at the tradeoff between security and network performance has been proposed to build reasonable trust relationship among sensor nodes, represented by numerical values, ie, trust values. In the work of Bao et al,[81] a cluster-based hierarchical trust management protocol for WSNs has been proposed to effectively deal with malicious nodes. This protocol considers multi-dimensional trust attributes derived from communication and social networks to evaluate the overall trust of a sensor node.

6 | PROTOCOL SUITE FOR IoT

IoT can be viewed as a global computer network of integrated technologies including WSNs, Global System for Mobile communication (GSM) and intelligent devices. IP based Internet is visualized to provide a flexible architecture to IoT. But limited computational capabilities and memory of the sensor devices are biggest challenge in the deployment of these devices. So in order to facilitate and simplify the accessibility of applications and services for these wireless and resource-constrained devices, the Internet Engineering Task Force (IETF) proposed a set of protocols and open standards including Constrained Application Protocol (CoAP) and 6LoWPAN. To develop large scale IoT applications, an appropriate understanding of the available standards and protocols, challenges associated with their large scale implementations, possible solutions to meet those challenges is required on per-layer basis. In addition, integrated working of these protocols is desired in order to deliver appropriate functionality. Details of some of the IoT protocols proposed by IETF are summarized in Table 4.[84,85] Table 5 provides a comparative analysis of ZigBee and WirelessHART.[86,87]

Integration of IPv6 based Internet and constrained network using these protocols is shown in Figure 11. IPv6 device can be either a personal computer or a smart phone, and it is accessing a remote wireless resource-constrained device like sensor through the HTTP-CoAP gateway using either wired or wireless connection. Other application layer protocols and standards for IoT include MQTT,[88] Advanced Message Queuing Protocol (AMQP),[89] and Data Distribution Service (DDS) standard.

7 | SOME OPEN SOURCE TOOLS AND DATASETS FOR IOT DEVELOPMENT

7.1 | Open source tools

A number of open source tools are available for the proliferation of the development and adoption of IoT-based applications. These tools help developers from start ups and well-established organizations to build new IoT devices and applications and thus act as the main driving force for IoT paradigm. They enable researchers to formulate theories, develop system models, and devise experimental results. Some of the widely used tool types, along with examples, are shown in Figure 12, and a brief description of each is given in Table 6.

TABLE 4 IETF Protocol Suite for IoT

IoT Architectural Layer(TCP/IP Layer)	Standards (Example Protocols)/Protocols	Specifications	Challenges	Existing Solutions
Perception Layer (Physical and Data Link Layer)	IEEE 802.15.4 (ZigBee, WirelessHART)	• Radio coverage is of few meters • Suitable for low power and low data rate applications • Maximum data rate = 250 kbps • Maximum output power = 1 mW	Limited channel capacity or Low channel rate which limits scalability and application load of IoT; Node congestion close to gateways in heavy traffic conditions	Time Slotted Channel Hopping (TSCH) MAC, Max Weight Scheduling (MWS)
		• Maximum packet size = 127 bytes	Energy insufficiency	Sensors operating in Duty Cycle Mode
		• Available space for upper layer protocols = Between 86 and 116 bytes • Radio power management	Heterogeneous co-existing traffic and poor QoS	Multiple transmission queues for different types of data
	6LoWPAN	• Minimum MTU = 1280 bytes • Develops scheme supporting mesh routing • Simplified IPv6 Neighbor Discovery Protocol (NDP), use cases and routing requirements	Availability of limited payload size for application layer due to smaller frame size and header overhead by lower layer protocols	Stateless compression, ie, LOWPAN_HC1 and LOWPAN_IPHC for IP header
			MTU supported by lower layer is smaller than that of IPv6	Segmentation of IPv6 packets by introducing an adaptation layer over data link layer
Transmission Layer (Network Layer)	ROLL - Routing Over Low power and Lossy networks (RPL - Routing Protocol for LLN)	• Distance vector routing protocol • Supports 3 kinds of traffic flow - ✓Point-to-Point ✓Point-to-Multipoint ✓Multipoint-to-Point	End-to-End throughput challenge due to co-existence of multiple applications in one physical network	Queue-aware backpressure routing algorithm; Opportunistic routing and networking encoding
		• Utilizes routing requirements and multiple quantitative metrics for nodes and links	Packet re-ordering due to multi-path routing structure	Load balancing[82]
			Effect of Duty Cycling on End-to-End latency; throughput delivery-ratio	Adaptive control on Duty Cycling[83]
			Increase in cost of DAG construction and maintenance due to multi-path routing and diverse traffic	Network optimization approach
Application Layer (Application Layer)	CoAP (Constrained Application Protocol)	• Constrained Web transfer protocol • Satisfies REST style • Supports built-in resource discovery • M2M compliant • Asynchronous message transfer • Datagram oriented (UDP – User Datagram Protocol) underlying transport and reliable unicast and multicast support • Stateless CoAP-HTTP and HTTP-CoAP mapping • Less header overhead • URI support • Proxy and caching	Resource scalability due to IP address update	Dynamic Domain Name System
			Network robustness in massive access situations	Caching mechanism
			Hardware cost Power Consumption	Mass production Observer/Subject mechanism

TABLE 5 ZigBee vs WirelessHART

Protocol→ Comparison Criterion↓	ZigBee	WirelessHART
Security	Not mandatory	Mandatory
Channel Frequency	Static Channel	Channel diversity due to Frequency Hoping
Frequency Interference	High	Low
Effect on breakage of Wireless link	New path is established as no alternate paths are available	Mesh networking provides alternate paths
Battery Powered Operations	Not suitable	Suitable
Backward Compatibility	Low	High
Scalability	Low	High

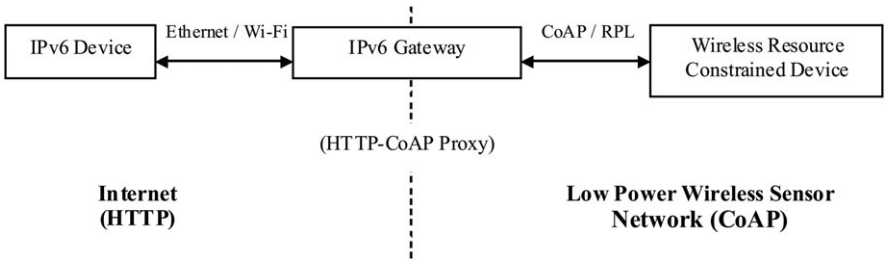

FIGURE 11 Integration of existing Internet devices with Constrained Network Devices through IETF Protocol Suite

Arduino is an open-source, cross-platform IoT development tool which contains an on-board microcontroller which is capable of performing a set of instructions over the input which can be either light sensed by the sensors or any text message, and results in output like turning on an LED, or posting the text message online on a social networking website. Instructions can be given to the microcontroller by using Arduino Programming Language which is based on Wiring, an open source programming platform; and Arduino Software which is based on Processing, a visual art based programming language.[90] *Eclipse IoT Project* provides open source technologies, tools, standards, protocols to the developers for developing IoT solutions for industries and consumers. A number of companies including IBM Redhat, Bosch are working collaboratively in supporting this project.[91]

BeagleBoards are low-cost, fan-less single-board computers based on low-power consumption. Their open source designs are available for developing compatible hardware.[92] *OpenPicus* is an Italian hardware company which provides open platform for the development of IoT devices and services.[93] *Arduino Ethernet Shield* provides Internet connectivity to the Arduino and enables it to send and receive data from anywhere across the globe.[94] *OpenIoT* is an open source middleware which utilizes efficient ways to integrate security, service delivery, Cloud Computing, and utility-based models to develop IoT solutions.[95] *IoTSys* is an open source integration middleware which provides gateway capabilities to the existing sensors and actuators in modern automation systems.[96] It also provides a stack which can be directly deployed over 6LoWPAN devices.

Raspberry Pi is a series of small credit card–sized Linux-based computers that provide desired functionalities at low-power consumption levels.[97] Arduino being a microcontroller motherboard, is capable of running single program at a time. On the other hand, Raspberry Pi is a general purpose computer which can execute multiple programs at a time. *Contiki* is an open source operating system for IoT which connects tiny low-cost, low-power microcontrollers to the Internet. It supports fully standard IPv4 and IPv6 along with recent low-power wireless standards – 6LowPAN,

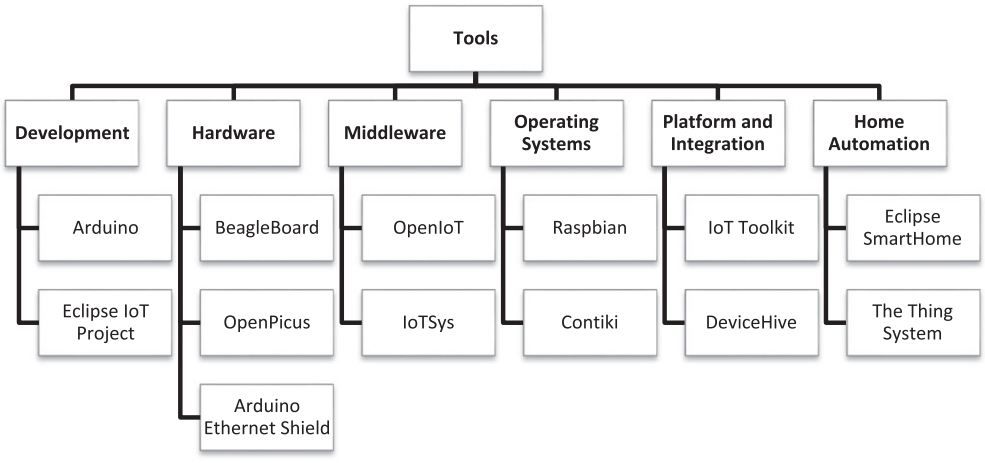

FIGURE 12 Open source tools for IoT

TABLE 6 Tools for IoT Environment

Tools	Examples	Description
IoT Development Tools	Arduino[90]	An open source electronics platform based on easy-to-use hardware and software.
	Eclipse IoT Project[91]	Provides the technology needed to build IoT devices, gateways, and Cloud platforms. Related projects include Paho, Mosquitto, Californium.
Hardware	BeagleBoard[92]	Offers credit-card sized computers having low power requirements that can run android and Linux.
	OpenPicus[93]	An Italian hardware company which develops IoT systems on programmable modules called Flyport.
	Arduino Ethernet Shield[94]	Connects Arduino to the Internet.
Middleware	OpenIoT[95]	Open Source middleware for getting information from sensor Clouds and offers utility-based IoT services.
	IoTSys[96]	Integration middleware for IoT which provides communication stack for embedded devices based on IPv6 and web services to establish interoperable interfaces for smart objects.
Operating Systems	Raspbian[97]	Raspberry Pi OS based on the Debian distribution of Linux.
	Contiki[98]	Connects low-power microcontrollers to the internet and supports standards like IPv6, 6LowPAN, and CoAP.
Platform & Integration Tools	IoT Toolkit[99,100]	Tools for integrating multiple IoT-related sensor networks and protocols.
	DeviceHive[101]	Provides an M2M communication framework for connecting devices to applications in IoT environment and enables users to visualize data from the devices.
Home Automation Software	Eclipse SmartHome[102]	A flexible framework designed to run on embedded devices such as Raspberry Pi.
	The Thing System[103]	Utilizes software and network protocols that enable users to control and fix the IoT devices

CoAP, and RPL.[98] *IoT Toolkit* is an open source project to develop a set of tools for building IoT gateways and service gateways that support multiple protocols in cooperation with multiple services. The project consists of the smart object API, gateway service, and other related tools.[99,100] *DeviceHive* is an open source M2M platform which provides building blocks to companies for developing or customizing their own M2M solutions for the IoT environment.[101] Home Automation Software like *Eclipse SmartHome*[102] and *The Thing System*[103] integrate devices, protocols, and application software for developing Smart home solutions.

7.2 | Open datasets for IoT

Many datasets are freely available on the Internet that are commonly used for experimentation and analysis purpose. These datasets enable developers to test the functionality of the analytical methods developed by them in order to improve and optimize the same. Most of the modern datasets are sensor-based, collected via Internet protocols, various applications and devices, and are related to weather, security incidents, transportation, healthcare domains, and so on. Table 7 gives a brief description of widely used datasets related to IoT environment that are available for public access.

8 | OPEN CHALLENGES AND FUTURE RESEARCH DIRECTIONS

8.1 | Standardized architecture

Since IoT is in its initial stages of development, its overall architecture will bring significant effects on its growth. A number of organizations across the globe have proposed IoT architectures on the basis of different perspectives, such as underlying technology, business models and services, or the application domain. For example, SENSEI,[110] an integrated project of European Union (EU), has developed an open and application driven IoT architecture which addresses scalability issues from globally distributed wireless sensor networks perspectives. Gubbi et al.[111] has proposed a Cloud-centric architecture in which user is the prime entity who can access data and infrastructure for developing new applications. Datta et al.[112] has proposed a gateway-centric architecture which allows real time intercommunication between mobile hosts and smart devices through wireless gateways to support novel M2M services including endpoint discovery, metadata reporting, configuration storage etc. Despite of all the researches made till date, no global standardization has been done for the IoT framework. Different security issues and application requirements have led to the development of abstract ideas. However, integrating the requirements and functionalities into a single full-fledge model which would serve the purpose for different applications is an open challenge.

TABLE 7 Dataset description

Datasets	Type	Description	Number of Instances
Linked Sensor Data (Kno.e.sis Center)[104]	Standalone Repository	For sensors and sensor observations created at Kno.e.sis Center; converted from weather data at Meoswest.	Contains descriptions of 20 thousand weather stations and 160 million observations
Japan Traffic Flow: cargo/passengers Flow [105]	Standalone Repository	A record of passenger and cargo aggregate by means of transportation within the nation as reported by Ministry of Land, Infrastructure, Transport and Tourism.	Passenger flow between 51 regions of the nation and cargo flow between 54 regions
Eurostat – European Commission[106]	Standalone Repository	Security Incidents against Information and Communication Technologies (ICT) and their consequences.	11680
NPTLab – Internet of people, things, and computers, User identification across multiple social sites[107]	Standalone Repository	Profile information of set of google+ users who make links to their Facebook or Twitter's profiles publicly available.	Dynamic
UCI Machine-Learning Repository[108]	Multi-Dataset Repository	Provides multi-purpose datasets including datasets for Air Quality, GPS trajectories, Wearable Computing etc.	Dynamic
The Community Resource for Archiving Wireless Data At Dartmouth (CRAWDAD)[109]	Multi-Dataset Repository	Provides data related to mobile devices or wireless networks including wireless contact traces, location of people using mobile phones, etc.	Dynamic

8.2 | Energy-efficient perception

Using multiple heterogeneous devices to sense data from the surroundings has direct implications on the traffic over the communication channels, data processing, data storage, and energy consumption of the devices.[111] To meet the competing demands of fixed nodes and infrastructure-less sensing environment simultaneously, a framework needs to be designed in order to efficiently exploit the data collection and storage capabilities by considering the energy consumption of the devices as well. A generalized energy-efficient modeling technique is required to map the collected data with respect to an appropriate application. Solar and Electromagnetic energy harvesting systems,[113] Analog sensing,[114] event-based data collection and traffic reduction scheme[115,116] are few novel energy efficient sensing techniques for large-scale WSNs. Compressive Wireless Sensing (CWS)[117] technique involves finding structural regularities among the sensed data that can be compressed, thereby reducing the transmission power of constrained sensor nodes.

8.3 | Security and privacy

Large-scale deployment of IoT networks would face major security and privacy issues. Due to resource constraints, smart devices are unable to support highly secure protocols and cryptographic algorithms. There are a number of ways in which these systems can be attacked. Key enabling technologies (RFID, WSN, Cloud, etc) in IoT are vulnerable to their own kind of attacks, including tracking of devices and objects, disclosure of the personal information, introduction of malicious data and code into the network, node compromise, selective opening attacks,[118] etc. Different solutions have been proposed in the past to deal with such kind of attacks. However, for large-scale implementation of networks, more research is required for these solutions to get widely accepted. The Secure Internet of Things Project (SITP) is a research initiative by faculty people of some of the well-known educational institutes in United States which focuses on user and application security in ubiquitous sensing environment through software and hardware analytics systems.[119] IoT Security Foundation (IoTSF), which was launched in 2015 in England, has started number of priority working groups that are focusing on trust establishment in IoT.[120] To ensure privacy, users must be aware of who is collecting their personal data, how it is getting collected, and how it is going to be used. Policy based mechanisms can be adopted to ensure privacy at end devices level.[121]

8.4 | Denial of service (DoS) attacks

Due to limited resources, smart devices are mainly focused on implementing the functionality rather than adapting the security features. This is one of the biggest reasons of these devices becoming a powerful means of major cyber attacks, one of which is DoS. New variants of DoS even go undetected unless there is a complete service breakdown. Mirai, Hajime, BrickerBot are some of the well-known and powerful IoT botnets that have targeted Internet-based services in the recent past. Although a number of mechanisms have been proposed in the literature to deal with DoS attacks, these efforts are not mature enough to deal with attacks in highly mobile environment of large number of heterogeneous devices. A number of

on-going researches are focusing on developing a new generation architecture of Internet. Named Data Networking (NDN) is one such approach based on Content-Centric Networking (CCN).[122]

8.5 | Quality of service (QoS)

With the rapid development of high capacity applications and services in IoT, QoS has become an important research area which requires more attention. IoT would support heterogeneous networks that would provide multiple services and distinct applications having different content types and QoS requirements. For example, there can be different application types, such as delay-sensitive, delay-tolerant, data intensive, noise sensitive, etc. Service incompatibility is common in different implementation environment. Therefore, an optimal approach to handle different traffic formats with different QoS requirements is required. Li et al[123] proposed a QoS-aware scheduling model for enhancing QoS in service-oriented architecture of IoT. Song et al[124] proposed a QoS-aware scheme to achieve energy efficiency in cluster-based industrial IoT systems. This scheme utilizes the concepts of Quantum Particle Swarm Optimization (QPSO) along with Genetic Algorithm (GA).

8.6 | Big data and data mining

Establishment of interconnectivity among billions of devices through Internet is going to generate huge amount of data, what is called Big data. Existing network infrastructures and software tools are unable to handle the same. Effective mechanisms are required for storing, retrieving and processing the bulk data. Utilizing a resource-constrained sensing environment for collecting data, using multiple layers of abstraction to interpret the large volume of collected data for extracting useful information out of it and mapping it to knowledge is a complex and challenging research problem. Current data mining techniques include shallow and deep learning,[125] supervised,[126-129] semi-supervised[130] and unsupervised learning, reinforcement learning, inference based learning, genetic learning, and so on.[111,131] There is a need to develop parallel and dynamic learning techniques in order to deal with complex events. Data stream mining for real-time processing and semantic reasoning are some of the future research areas for Cloud based IoT environment.

8.7 | Cloud computing

Cloud Computing technology in integration with IoT will enhance the development of smart applications that would support a large number of users and collaborative services provided by multiple stakeholders in a reliable manner.[132,133] Cloud platform must support the rapid growth of the number of applications that utilize the capabilities of heterogeneous resources in order to ensure QoS to the end users. These applications must be able to operate in constrained wired and wireless environment. Real-time applications must be executed in parallel on different resources so that if any of the resource fails, processing should not halt. Resource scheduling should be performed in such a way so that critical real time tasks can be prioritize dynamically.

8.8 | Ongoing international efforts

Various stakeholders from industrial organizations, academia, and government are working collaboratively at global level in activities for the realization of IoT. The ITU-T Focus Group on Data Processing and Management (FG-DPM) was established in March 2017 in Dubai by ITU-T Study Group 20 to support IoT-based Smart Cities and Communities. IETF is working on transport layer security and low power wireless PANs and many other application layer protocols. Similarly, other such Alliances and Consortiums that are working in the field of IoT and its related technologies are OASIS, International Standard Organization (ISO), UPnP, IoT Eclipse, and the Open Interconnect Consortium (OIC). World Smart City Community is working on Smart City projects across many nations, including United States, UK, Japan, Korea, and Australia. Government of India has initiated a Smart City Mission in the year 2015, which is a 5-year program to develop citizen friendly and smart core infrastructure of 100 cities in the nation.

9 | CONCLUSION

Internet has significantly changed our lives and was built across host-to-host communications in order to provide information services. IoT has evolved as an emerging paradigm which will establish connectivity between anything and anytime. Proliferation of smart devices having sensing and communication capabilities has been attracting a significant interest in the field. However, with these rapid advancements come all kinds of challenges associated with the field as well as its supporting technologies.

In this paper, we started with the historical background of IoT and highlighted some of the major events associated with its growth since the term came into existence. We also covered some of the statistics and predictions related to the field. We discussed the security architecture of IoT in detail which consists of 3 layers – Perception layer, Transmission layer, and Application layer. Key features and technologies associated with each layer have been analyzed. Perception layer utilizes sensory and identification technologies such as RFID, WSN, and GPS that gather information from the surroundings and forward it to the gateways. Transmission layer is responsible for establishing the communication infrastructure so that end users can access Internet-based services. Application layer consists of application support layer and numerous IoT applications and involves the

use of handheld devices and terminals to provide application accessibility to the users. It is through application layer that end users interact with IoT environment.

An analysis has been made on the challenges associated with IoT architecture, elements of the IoT environment, its enabling technologies, and featured characteristics, along with some of the existing solutions. We also analyzed challenges and existing solutions specific to RFID and WSNs that are the key enabling technologies for this domain. Some of the key protocols developed by IETF community, their specifications, implementation advantages and challenges, existing solutions, along with a comparison on ZigBee and WirelessHART, have been presented. Some of the open source tools and datasets for IoT development and research have also been covered. The paper has been concluded with some open research issues, ongoing research activities, and future possibilities in order to give an insight of the possible work directions in the field to overcome the existing and upcoming challenges.

ACKNOWLEDGMENT

This research work is being supported by Project grant (SB/FTP/ETA-131/2014) from SERB, DST, Government of India.

ORCID


B.B. Gupta http://orcid.org/0000-0003-4929-4698

REFERENCES

1. Yan Z, Zhang P, Vasilakos AV. A survey on trust management for Internet of Things. *J Netw Comput Appl*. 2014;42:120-134.
2. Li S, Da Xu L, Zhao S. The Internet of Things: a survey. *Inf Syst Front*. 2015;17(2):243-259.
3. Granjal J, Monteiro E, Silva JS. Security for the Internet of Things: a survey of existing protocols and open research issues. *IEEE Commun Surv Tutor*. 2015;17(3):1294-1312.
4. Ngu AH, Gutierrez M, Metsis V, Nepal S, Sheng QZ. IoT middleware: a survey on issues and enabling technologies. *IEEE Internet Things J*. 2017;4(1):1-20.
5. Adat V, Gupta BB. Security in Internet of Things: issues, challenges, taxonomy, and architecture. *Telecommun Syst*. 2018;67(3):423-441.
6. Ashton K. That 'Internet of Things' Thing. *RFID J*. 2011.
7. InformationWeek. Internet of Things Done Wrong Stifles Innovation. http://www.informationweek.com/strategic-cio/executive-insights-and-innovation/internet-of-things-done-wrong-stifles-innovation/. Published July 7, 2014. Accessed June 2017.
8. Weiser M. The computer for the 21st century. *Sci Am*. 1991;265(3):94-105.
9. Mattern F, Floerkemeier C. From the Internet of Computers to the Internet of Things. In: *From Active Data Management to Event-Based Systems and More*. Berlin, Germany: Springer-Verlag Berlin Heidelberg; 2010;242-259.
10. MQTT.ORG. http://mqtt.org/. Accessed July 2017.
11. Internet.org. https://info.internet.org/. Accessed July 2017.
12. IoT One. https://www.iotone.com/. Accessed July 2017.
13. Coetzee L, Eksteen J. The Internet of Things-promise for the future? An introduction. Paper presented at: IST-Africa Conference Proceedings; 2011; Gaborone, Botswana.
14. Evans D. The Internet of Things: How the Next Evolution of the Internet is Changing Everything. CISCO White Paper. San Jose, CA: CISCO; 2011:1-11.
15. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of Things: a survey on enabling technologies, protocols, and applications. *IEEE Commun Surv Tutor*. 2015;17(4):2347-2376.
16. Floyer D. *Defining and Sizing the Industrial Internet*. Marlborough, MA: Wikibon; 2013.
17. Dunbrack L, Ellis S, Hand L, Knickle K, Turner V. IoT and Digital Transformation: A Tale of Four Industries. IDC White Paper. Framingham, MA: International Data Corporation; 2016.
18. ITU-T, Y. Overview of ubiquitous networking and of its support in NGN. ITU-T Recommendation; 2009.
19. IEEE Standards Association. P2413-Standard for an Architectural Framework for the Internet of Things (IoT). New York, NY: Institute of Electrical and Electronics Engineers; 2016.
20. Krco S, Pokric B, Carrez F. Designing IoT architecture (s): a European perspective. Paper presented at: IEEE World Forum on Internet of Things (WF-IoT); 2014 Seoul, South Korea.
21. Jing Q, Vasilakos AV, Wan J, Lu J, Qiu D. Security of the Internet of Things: perspectives and challenges. *Wirel Netw*. 2014;20(8):2481-2501.
22. Suo H, Wan J, Zou C, Liu J. Security in the Internet of Things: a review. Paper presented at: 2012 Computer Science and Electronics Engineering (ICCSEE); 2012; Hangzhou, China.
23. Khan R, Khan SU, Zaheer R, Khan S. Future internet: the Internet of Things architecture, possible applications and key challenges. Paper presented at: 10th International Conference on Frontiers of Information Technology (FIT); 2012; Islamabad Pakistan.
24. Wu M, Lu TJ, Ling FY, Sun J, Du HY. Research on the architecture of Internet of things. Paper presented at: 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE); 2010; Chengdu, China.
25. Li C, Chen CL. A multi-stage control method application in the fight against phishing attacks. In: Proceeding of the 26th computer security academic communication across the country; 2011.
26. Alaba FA, Othman M, Hashem IAT, Alotaibi F. Internet of Things security: a survey. *J Netw Comput Appl*. 2017;88:10-28.
27. Raza U, Kulkarni P, Sooriyabandara M. Low power wide area networks: an overview. *IEEE Commun Surv Tutor*. 2017;19(2):855-873.

28. Iraji S, Mogensen P, Ratasuk R. Recent advances in M2M communications and Internet of Things (IoT). *Int J Wirel Inf Netw*. 2017;24(3):240-242.
29. Ferrera E, Conzon D, Brizzi P, et al. XMPP-based infrastructure for IoT network management and rapid services and applications development. *Ann Telecommun*. 2017;72(7-8):443-457.
30. Ndiaye M, Hancke GP, Abu-Mahfouz AM. Software defined networking for improved wireless sensor network management: a survey. *Sensors*. 2017);17(5):1031.
31. Semasinghe P, Maghsudi S, Hossain E. Game theoretic mechanisms for resource management in massive wireless IoT systems. *IEEE Commun Mag*. 2017;55(2):121-127.
32. Chen R, Guo J, Bao F. Trust management for SOA-based IoT and its application to service composition. *IEEE Trans Serv Comput*. 2016;9(3):482-495.
33. Krishna MB. Security and trust management for the Internet of Things: an RFID and sensor network perspective. In: *Cyber-Assurance for the Internet of Things*. Hoboken, NJ: John Wiley & Sons Inc; 2016;137-162.
34. The Register. Today the web was broken by countless hacked devices. https://www.theregister.co.uk. Published October 21, 2016. Accessed June 2017.
35. Massis B. The Internet of Things and its impact on the library. *New Libr World*. 2016;117(3/4):289-292.
36. Mejri MN, Ben-Othman J, Hamdi M. Survey on VANET security challenges and possible cryptographic solutions. *Veh Commun*. 2014;1(2):53-66.
37. Moosavi SR, Gia TN, Rahmani A-M, et al. SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Comput Sci*. 2015;52:452-459.
38. Lu C. Overview of security and privacy issues in the Internet of Things. *Internet Things (IoT) Vis Archit Elem Future Dir*; 2014.
39. Lee C, Zappaterra L, Choi K, Choi HA. Securing smart home: technologies, security challenges, and security requirements. Paper presented at: IEEE Conference on Communications and Network Security (CNS); 2014; San Francisco, CA.
40. Perera C, Zaslavsky A, Christen P, Georgakopoulos D. Context aware computing for the Internet of Things: a survey. *IEEE Commun Surv Tutor*. 2014;16(1):414-454.
41. Zhang Y, Shen Y, Wang H, Yong J, Jiang X. On secure wireless communications for IoT under eavesdropper collusion. *IEEE Trans Autom Sci Eng*. 2016;13(3):1281-1293.
42. Komninos N, Philippou E, Pitsillides A. Survey in smart grid and smart home security: issues, challenges and countermeasures. *IEEE Commun Surv Tutor*. 2014;16(4):1933-1954.
43. Bekara C. Security issues and challenges for the IoT-based smart grid. *Procedia Comput Sci*. 2014;34:532-537.
44. Aman W, Snekkenes E. Managing security trade-offs in the internet of things using adaptive security. Paper presented at: 10th International Conference for Internet Technology and Secured Transactions (ICITST); 2015; London, UK.
45. Djahel S, Doolan R, Muntean GM, Murphy J. A communications-oriented perspective on traffic management systems for smart cities: challenges and innovative approaches. *IEEE Commun Surv Tutor*. 2015;17(1):125-151.
46. Olawumi O, Väänänen A, Haataja K, Toivanen P. Security issues in smart home and mobile health system: threat analysis, possible countermeasures and lessons learned. *Int J Inf Technol Secur*. 2017;9(1):31-52.
47. Ziegler S, Crettaz C, Ladid L, et al. IoT6–moving to an IPV6-based future IoT. In: *The Future Internet Assembly*. Berlin, Germany: Springer; 2013:161-172.
48. Jia X, Feng Q, Fan T, Lei Q. RFID technology and its applications in Internet of Things (IoT). Paper presented at: 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet); 2012; Yichang, China.
49. Juels A. RFID security and privacy: a research survey. *IEEE J Sel Areas Commun*. 2006;24(2):381-394.
50. Kulkarni G, Sutar R, Mohite S. RFID security issues & challenges. Paper presented at: International Conference on Electronics and Communication Systems (ICECS); 2014; Coimbatore, India.
51. Lakafosis V, Traille A, Lee H, et al. RFID-CoA: the RFID tags as certificates of authenticity. Paper presented at: 2011 IEEE International Conference on RFID (RFID); 2011; Orlando, FL.
52. Alotaibi M, Postula A, Portmann M. Tag anti-collision algorithms in RFID systems-a new trend. *WSEAS Trans Commun*. 2009;8(12):1216-1232.
53. Myung J, Lee W, Srivastava J. Adaptive binary splitting for efficient RFID tag anti-collision. *IEEE Commun Lett*. 2006;10(3):144-146.
54. Ryu J, Lee H, Seok Y, Kwon T, Choi Y. A hybrid query tree protocol for tag collision arbitration in RFID systems. Paper presented at: IEEE International Conference on Communications (ICC); 2007; Glasgow, Scotland.
55. Wang K-H, Chen C-M, Fang W, Wu T-Y. On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags. *J Supercomput*. 2018;74(1):65-70.
56. Ohkubo M., Suzuki K, Kinoshita S. Efficient hash-chain based RFID privacy protection scheme. Paper presented at: International Conference on Ubiquitous Computing-Ubicomp, Workshop Privacy: Current Status and Future Directions; 2004.
57. Juels A, Weis SA. Defining strong privacy for RFID. *ACM Trans Inf Syst Secur (TISSEC)*. 2009;13(1):7.
58. Juels A, Rivest RL, Szydlo M. The blocker tag: selective blocking of RFID tags for consumer privacy. In: Proceedings of the 10th ACM Conference on Computer and Communications Security; 2003; Washington, DC.
59. Ateniese G, Camenisch J, De Medeiros B. Untraceable RFID tags via insubvertible encryption. In: Proceedings of the 12th ACM Conference on Computer and Communications Security; 2005; Alexandria, VA.
60. Periaswamy SCG, Thompson DR, Di J. Fingerprinting RFID tags. *IEEE Trans Dependable Secure Comput*. 2011;8(6):938-943.
61. Yao Q, Qi Y, Han J, Zhao J, Li X, Liu Y. Randomizing RFID private authentication. Paper presented at: Seventh Annual IEEE International Conference on Pervasive Computing and Communications (PerCom); 2009; Galveston, TX.
62. Sadighian A, Jalili R. AFMAP: anonymous forward-secure mutual authentication protocols for RFID systems. Paper presented at: Third International Conference on Emerging Security Information, Systems and Technologies (SECURWARE); 2009; Athens/Glyfada, Greece.
63. Hoque ME, Rahman F, Ahamed SI. AnonPri: an efficient anonymous private authentication protocol. Paper presented at: IEEE International Conference on Pervasive Computing and Communications (PerCom); 2011; Seattle, WA.
64. Christin D, Reinhardt A, Mogre PS, Steinmetz R. Wireless sensor networks and the Internet of Things: selected challenges. In: Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose Sensornetze; 2009; Hamburg, Germany.

65. Roman R, Lopez J. Integrating wireless sensor networks and the internet: a security analysis. *Internet Res*. 2009;19(2):246-259.
66. Ganeriwal S, Srivastava MB. Reputation-based framework for high integrity sensor networks. In: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN); 2004; Washington, DC.
67. Pu CC, Chung WYC. Group key update method for improving RC4 stream cipher in wireless sensor networks. Paper presented at: International Conference on Convergence Information Technology; 2007; Gyeongju, South Korea.
68. Kukkurainen J, Soini M, Sydänheimo L. RC5-based security in wireless sensor networks: utilization and performance. *WSEAS Trans Comput*. 2010;9(10):1191-1200.
69. Ding Y. Key management scheme for WSN using ECC. *J Xidian Univ*. 2008;4:029.
70. Murphy G, Keeshan A, Agarwal R, Popovici E. Hardware-software implementation of public-key cryptography for wireless sensor networks. Paper presented at: IET Irish Signals and Systems Conference; 2006; Dublin, Ireland.
71. Shen J, Gui Z, Ji S, Shen J, Tan H, Tang Y. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. *J Netw Comput Appl*. 2018;106:117-123.
72. Li J, Sun L, Yan Q, Li Z, Srisa-an W, Ye H. Significant permission identification for machine learning based android malware detection. *IEEE Trans Ind Inform*. 2018.
73. Gaubatz G, Kaps JP, Ozturk E, Sunar B. State of the art in ultra-low power public key cryptography for wireless sensor networks. Paper presented at: Third IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom); 2005; Kauai Island, HI.
74. Eschenauer L, Gligor VD. A key-management scheme for distributed sensor networks. In: Proceedings of the 9th ACM Conference on Computer and Communications Security; 2002; Washington, DC.
75. Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. In: Proceedings of the 2003 Symposium on Security and Privacy; 2003; Berkeley, CA.
76. Akkaya K, Younis M. A survey on routing protocols for wireless sensor networks. *Ad Hoc Netw*. 2005;3(3):325-349.
77. Heinzelman WR, Kulik J, Balakrishnan H. Adaptive protocols for information dissemination in wireless sensor networks. In: Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking; 1999; Seattle, WA.
78. Heinzelman WR, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks. In: Proceedings of the 33rd Annual Hawaii International Conference on System Sciences; 2000; Maui, HI.
79. Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Netw*. 2003;1(2):293-315.
80. Yao Z, Kim D, Lee I, Kim K, Jang J. A security framework with trust management for sensor networks. Paper presented at: Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks; 2005; Athens, Greece.
81. Bao F, Chen R, Chang M, Cho JH. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. *IEEE Trans Netw Serv Manag*. 2012;9(2):169-183.
82. Kandula S, Katabi D, Sinha S, Berger A. Dynamic load balancing without packet reordering. *ACM SIGCOMM Comput Commun Rev*. 2007;37(2):51-62.
83. Vigorito CM, Ganesan D, Barto AG. Adaptive control of duty cycling in energy-harvesting wireless sensor networks. In: Proceedings of the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON); 2007; San Diego, CA.
84. Sheng Z, Yang S, Yu Y, Vasilakos A, Mccann J, Leung K. A survey on the IEFT protocol suite for the Internet of Things: standards, challenges, and opportunities. *IEEE Wirel Commun*. 2013;20(6):91-98.
85. Palattella MR, Accettura N, Vilajosana X, et al. Standardized protocol stack for the Internet of (important) Things. *IEEE Commun Surv Tutor*. 2013;15(3):1389-1406.
86. Lennvall T, Svensson S, Hekland F. A comparison of WirelessHART and ZigBee for industrial applications. Paper presented at: IEEE International Workshop on Factory Communication Systems (WFCS); 2008; Dresden, Germany.
87. Habib G, Haddad N, El Khoury R. Case study: WIRELESSHART vs ZIGBEE network. Paper presented at: Third International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE); 2015; Hadeth, Lebanon.
88. Hunkeler U, Truong HL, Stanford-Clark A. MQTT-S—a publish/subscribe protocol for wireless sensor networks. Paper presented at: 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE); 2008; Bangalore, India.
89. Kramer J. Advanced message queuing protocol (AMQP). *Linux J*. 2009;2009(187):3.
90. Arduino. An open-source electronics platform. https://www.arduino.cc/en/Main/Products. Accessed June 2017.
91. IoT Eclipse Project. https://iot.eclipse.org/projects/. Accessed June 2017.
92. BeagleBoard. Open source computing. https://beagleboard.org/. Accessed June 2017.
93. OpenPicus. Flyport: professional IoT modules. http://www.openpicus.com/. Accessed June 2017.
94. Arduino Ethernet Shield. https://www.arduino.cc/en/Main/ArduinoEthernetShield. Accessed June 2017.
95. OpenIoT. Open source cloud solution for Internet of Things. http://www.openiot.eu/. Accessed June 2017.
96. TU Wien: Technische Universität Wien. IoTSys - Internet of Things Integration Middleware. http://www.iue.tuwien.ac.at/cse/index.php/projects/120-iotsys-internet-of-things-integration-middleware.html. Accessed June 2017.
97. Raspbian. https://www.raspberrypi.org/downloads/raspbian/. Accessed June 2017.
98. Contiki. Open Source Operating System for Internet of Things. http://www.contiki-os.org/. Accessed June 2017.
99. Make. http://makezine.com/2014/02/05/the-internet-of-things-what-is-the-iot-toolkit/. Accessed June 2017.
100. IoT Toolkit. Reference implementation of the smart object API. http://iot-toolkit.com/. Accessed June 2017.
101. Device Hive. https://devicehive.com/. Accessed September 2017.
102. Eclipse SmartHome. A flexible framework for the smart home. https://eclipse.org/smarthome/. Accessed June 2017.
103. The Thing System. http://thethingsystem.com/index.html. Accessed September 2017.
104. Datahub. https://datahub.io/dataset/knoesis-linked-sensor-data. Accessed September 2017.

105. National Land Numeric Information. http://nlftp.mlit.go.jp/ksj-e/jpgis/datalist/KsjTmplt-S05-d.html. Accessed September 2017.
106. Eurostat. http://ec.europa.eu/eurostat/web/products-datasets/-/isoc_cisce_ic. Accessed September 2017.
107. Internet of People, Things and Computers. NPTLab. http://nptlab.di.unimi.it/?page_id=360. Accessed September 2017.
108. UCI. Machine Learning Repository. http://archive.ics.uci.edu/ml/datasets.html. Accessed September 2017.
109. Crawdad. http://crawdad.org/. Accessed August 2017.
110. SENSEI, Integrated EU Project - 7th Framework. http://www.ict-sensei.org/index.php. Accessed August 2017.
111. Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of things (IoT): a vision, architectural elements, and future directions. *Future Gener Comput Syst*. 2013;29(7):1645-1660.
112. Datta SK, Bonnet C, Nikaein N. An IoT gateway centric architecture to provide novel M2M services. Paper presented at: IEEE World Forum on Internet of Things (WF-IoT); 2014; Seoul, South Korea.
113. Bito J, Bahr R, Hester JG, Nauroze SA, Georgiadis A, Tentzeris MM. A novel solar and electromagnetic energy harvesting system with a 3-D printed package for energy efficient Internet-of-Things wireless sensors. *IEEE Trans Microw Theory Tech*. 2017;65(5):1831-1842.
114. Sadhu V, Zhao X, Pompili D. Energy-efficient analog sensing for large-scale, high-density persistent wireless monitoring. Paper presented at: 13th Annual Conference on Wireless On-demand Network Systems and Services (WONS); 2017; Jackson, WY.
115. Tiwari V, Keskar A, Shivaprakash NC. A reconfigurable IoT architecture with energy efficient event-based data traffic reduction scheme. *Int J Online Eng*. 2017;13(2):34-52.
116. Dong M, Ota K, Liu A. RMER: reliable and energy-efficient data collection for large-scale wireless sensor networks. *IEEE Internet Things J*. 2016;3(4):511-519.
117. Bajwa W, Haupt J, Sayeed A, Nowak R. Compressive wireless sensing. In: Proceedings of the 5th International Conference on Information Processing in Sensor Networks; 2006; Nashville, TN.
118. Huang Z, Liu S, Mao X, Chen K, Li J. Insight of the protection for data security under selective opening attacks. *Inf Sci*. 2017;412:223-241.
119. Stanford. Secure Internet of Things Project. http://iot.stanford.edu/. Accessed September 2017.
120. IoT Security Foundation. https://iotsecurityfoundation.org/. Accessed September 2017.
121. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: the road ahead. *Comput Netw*. 2015;76:146-164.
122. AbdAllah EG, Zulkernine M, Hassanein HS. DADI: defending against distributed denial of service in information-centric networking routing and caching. *Secur Priv*. 2018;1(2):e16.
123. Li L, Li S, Zhao S. QoS-aware scheduling of services-oriented Internet of Things. *IEEE Trans Ind Inform*. 2014;10(2):1497-1505.
124. Song L, Chai KK, Chen Y, Schormans J, Loo J, Vinel A. QoS-aware energy-efficient cooperative scheme for cluster-based IoT systems. *IEEE Syst J*. 2017;11(3):1447-1455.
125. Li P, Li J, Huang Z, et al. Multi-key privacy-preserving deep learning in cloud computing. *Future Gener Comput Syst*. 2017;74:76-85.
126. Chang X, Yu YL, Yang Y, Xing EP. Semantic pooling for complex event analysis in untrimmed videos. *IEEE Trans Pattern Anal Mach Intell*. 2017;39(8):1617-1632.
127. Li Z, Nie F, Chang X, Yang Y. Beyond trace ratio: weighted harmonic mean of trace ratios for multiclass discriminant analysis. *IEEE Trans Knowl Data Eng*. 2017;29(10):2100-2110.
128. Chang X, Ma Z, Yang Y, Zeng Z, Hauptmann AG. Bi-level semantic representation analysis for multimedia event detection. *IEEE Trans Cybern*. 2017;47(5):1180-1197.
129. Chang X, Ma Z, Lin M, Yang Y, Hauptmann AG. Feature interaction augmented sparse learning for fast kinect motion detection. *IEEE Trans Image Process*. 2017;26(8):3911-3920.
130. Chang X, Yang Y. Semisupervised feature analysis by mining correlations among multiple tasks. *IEEE Trans Neural Netw Learn Syst*. 2017;28(10):2294-2305.
131. Kim H-Y, Kim J-M. A load balancing scheme based on deep-learning in IoT. *Clust Comput*. 2017;20(1):873-878.
132. Cai H, Xu B, Jiang L, Vasilakos AV. IoT-based big data storage systems in cloud computing: perspectives and challenges. *IEEE Internet Things J*. 2017;4(1):75-87.
133. Theoharidou M, Tsalis N, Gritzalis D. Smart home solutions for healthcare: privacy in ubiquitous computing infrastructures. In: *Handbook of smart homes, health care and well-being*. Cham, Switzerland. Springer International Publishing; 2014.

How to cite this article: Gupta BB, Quamara M. An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency Computat Pract Exper*. 2018;e4946. https://doi.org/10.1002/cpe.4946