Journal of Big Data

SURVEY PAPER Open Access

Internet of Things is a revolutionary approach for future technology enhancement: a review

Sachin Kumar[1*], Prayag Tiwari[2] and Mikhail Zymbler[1]

*Correspondence: sachinagnihotri16@gmail.com
[1] Department of Computer Science, South Ural State University, Chelyabinsk, Russian Federation
Full list of author information is available at the end of the article

Abstract

Internet of Things (IoT) is a new paradigm that has changed the traditional way of living into a high tech life style. Smart city, smart homes, pollution control, energy saving, smart transportation, smart industries are such transformations due to IoT. A lot of crucial research studies and investigations have been done in order to enhance the technology through IoT. However, there are still a lot of challenges and issues that need to be addressed to achieve the full potential of IoT. These challenges and issues must be considered from various aspects of IoT such as applications, challenges, enabling technologies, social and environmental impacts etc. The main goal of this review article is to provide a detailed discussion from both technological and social perspective. The article discusses different challenges and key issues of IoT, architecture and important application domains. Also, the article bring into light the existing literature and illustrated their contribution in different aspects of IoT. Moreover, the importance of big data and its analysis with respect to IoT has been discussed. This article would help the readers and researcher to understand the IoT and its applicability to the real world.

Keywords: Internet of Things (IoT), IoT architecture, IoT challenges, IoT applications

Introduction

The Internet of Things (IoT) is an emerging paradigm that enables the communication between electronic devices and sensors through the internet in order to facilitate our lives. IoT use smart devices and internet to provide innovative solutions to various challenges and issues related to various business, governmental and public/private industries across the world [1]. IoT is progressively becoming an important aspect of our life that can be sensed everywhere around us. In whole, IoT is an innovation that puts together extensive variety of smart systems, frameworks and intelligent devices and sensors (Fig. 1). Moreover, it takes advantage of quantum and nanotechnology in terms of storage, sensing and processing speed which were not conceivable beforehand [2]. Extensive research studies have been done and available in terms of scientific articles, press reports both on internet and in the form of printed materials to illustrate the potential effectiveness and applicability of IoT transformations. It could be utilized as a preparatory work before making novel innovative business plans while considering the security, assurance and interoperability.

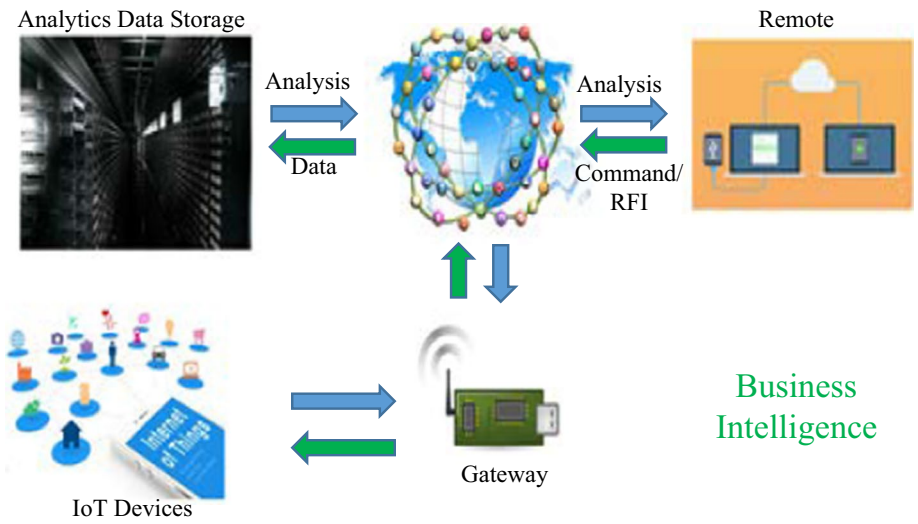

Fig. 1 General architecture of IoT

A great transformation can be observed in our daily routine life along with the increasing involvement of IoT devices and technology. One such development of IoT is the concept of Smart Home Systems (SHS) and appliances that consist of internet based devices, automation system for homes and reliable energy management system [3]. Besides, another important achievement of IoT is Smart Health Sensing system (SHSS). SHSS incorporates small intelligent equipment and devices to support the health of the human being. These devices can be used both indoors and outdoors to check and monitor the different health issues and fitness level or the amount of calories burned in the fitness center etc. Also, it is being used to monitor the critical health conditions in the hospitals and trauma centers as well. Hence, it has changed the entire scenario of the medical domain by facilitating it with high technology and smart devices [4, 5]. Moreover, IoT developers and researchers are actively involved to uplift the life style of the disabled and senior age group people. IoT has shown a drastic performance in this area and has provided a new direction for the normal life of such people. As these devices and equipment are very cost effective in terms of development cost and easily available within a normal price range, hence most of the people are availing them [6]. Thanks to IoT, as they can live a normal life. Another important aspect of our life is transportation. IoT has brought up some new advancements to make it more efficient, comfortable and reliable. Intelligent sensors, drone devices are now controlling the traffic at different signalized intersections across major cities. In addition, vehicles are being launched in markets with pre-installed sensing devices that are able to sense the upcoming heavy traffic congestions on the map and may suggest you another route with low traffic congestion [7]. Therefore IoT has a lot to serve in various aspects of life and technology. We may conclude that IoT has a lot of scope both in terms of technology enhancement and facilitate the humankind.

IoT has also shown its importance and potential in the economic and industrial growth of a developing region. Also, in trade and stock exchange market, it is being considered as a revolutionary step. However, security of data and information is an

important concern and highly desirable, which is a major challenging issue to deal with [5]. Internet being a largest source of security threats and cyber-attacks has opened the various doors for hackers and thus made the data and information insecure. However, IoT is committed to provide the best possible solutions to deal with security issues of data and information. Hence, the most important concern of IoT in trade and economy is security. Therefore, the development of a secure path for collaboration between social networks and privacy concerns is a hot topic in IoT and IoT developers are working hard for this.

The remaining part of the article is organized as follows: "Literature survey" section will provide state of art on important studies that addressed various challenges and issues in IoT. "IoT architecture and technologies" section discussed the IoT functional blocks, architecture in detail. In "Major key issues and challenges of IoT" section, important key issues and challenges of IoT is discussed. "Major IoT applications" section provides emerging application domains of IoT. In "Importance of big data analytics in IoT" section, the role and importance of big data and its analysis is discussed. Finally, the article concluded in "Conclusions" section.

Literature survey

IoT has a multidisciplinary vision to provide its benefit to several domains such as environmental, industrial, public/private, medical, transportation etc. Different researchers have explained the IoT differently with respect to specific interests and aspects. The potential and power of IoT can be seen in several application domains. Figure 2 illustrates few of the application domains of IoTs potentials.

Various important IoT projects have taken charge over the market in last few years. Some of the important IoT projects that have captured most of the market are shown in Fig. 3. In Fig. 3, a global distribution of these IoT projects is shown among American, European and Asia/Pacific region. It can be seen that American continent are contributing more in the health care and smart supply chain projects whereas contribution of European continent is more in the smart city projects [8].

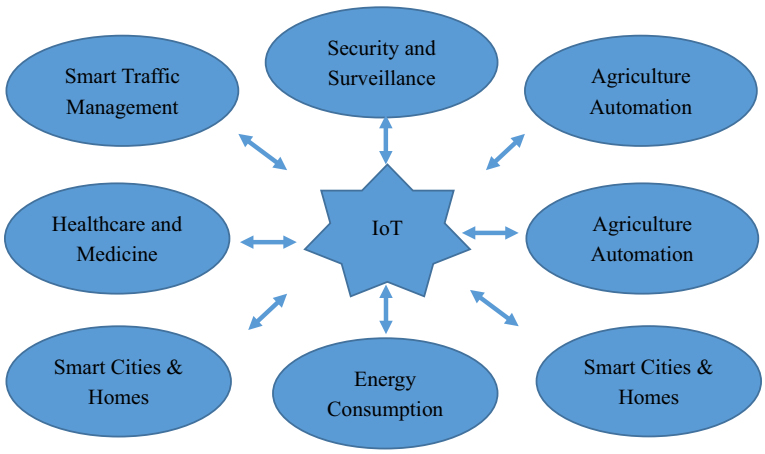

Fig. 2 Some of the potential application domains of IoT

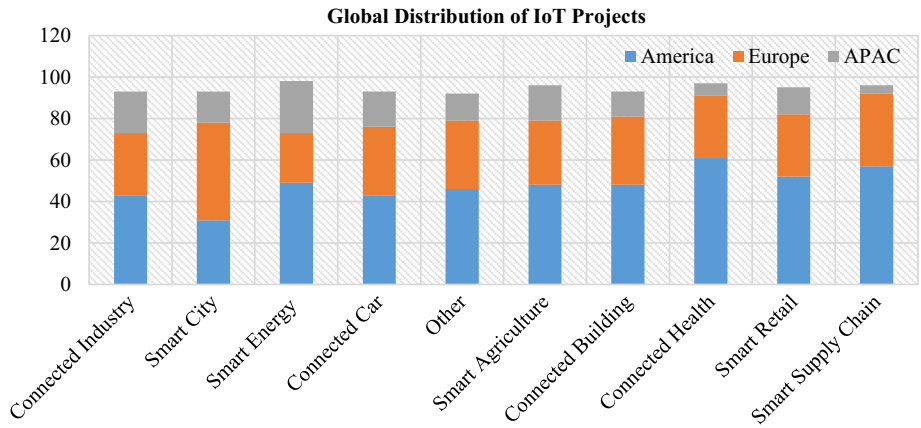

Fig. 3 Global distribution of IoT projects among America (USA, South America and Canada), Europe and APAC (Asia and Pacific region) [8]

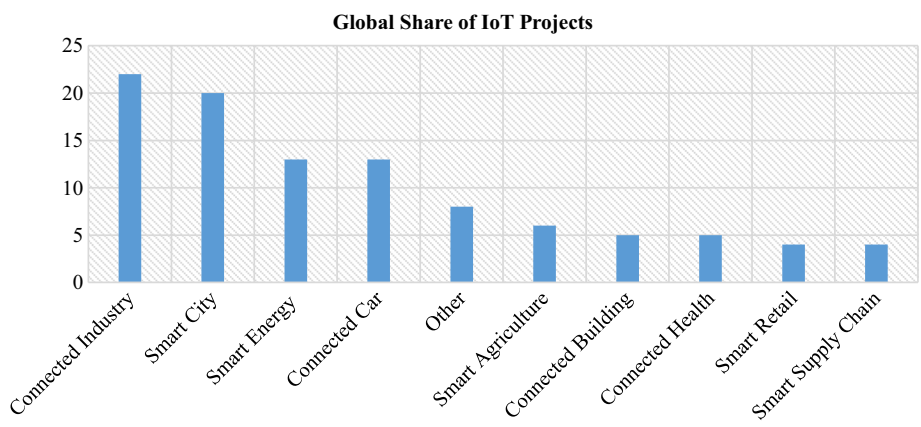

Fig. 4 Global share of IoT projects across the world [8]

Figure 4, illustrates the global market share of IoT projects worldwide [8]. It is evident that industry, smart city, smart energy and smart vehicle based IoT projects have a big market share in comparison to others.

Smart city is one of the trendy application areas of IoT that incorporates smart homes as well. Smart home consists of IoT enabled home appliances, air-conditioning/heating system, television, audio/video streaming devices, and security systems which are communicating with each other in order to provide best comfort, security and reduced energy consumption. All this communication takes place through IoT based central control unit using Internet. The concept of smart city gained popularity in the last decade and attracted a lot of research activities [9]. The smart home business economy is about to cross the 100 billion dollars by 2022 [10]. Smart home does not only provide the in-house comfort but also benefits the house owner in cost cutting in several aspects i.e. low energy consumption will results in comparatively lower electricity bill. Besides smart homes, another category that comes within smart city is smart vehicles. Modern cars are equipped with intelligent devices and sensors that control most of the components from the headlights of the car to the engine [11]. The IoT is committed towards

developing a new smart car systems that incorporates wireless communication between car-to-car and car-to-driver to ensure predictive maintenance with comfortable and safe driving experience [12].

Khajenasiri et al. [10] performed a survey on the IoT solutions for smart energy control to benefit the smart city applications. They stated that at present IoT has been deployed in very few application areas to serve the technology and people. The scope of IoT is very wide and in near future IoT is able to capture almost all application areas. They mentioned that energy saving is one of the important part of the society and IoT can assist in developing a smart energy control system that will save both energy and money. They described an IoT architecture with respect to smart city concept. The authors also discussed that one of the challenging task in achieving this is the immaturity of IoT hardware and software. They suggested that these issues must be resolved to ensure a reliable, efficient and user friendly IoT system.

Alavi et al. [13] addressed the urbanization issue in the cities. The movement of people from rural to urban atmosphere resulting in growing population of the cities. Therefore, there is a need to provide smart solutions for mobility, energy, healthcare and infrastructure. Smart city is one of the important application areas for IoT developers. It explores several issues such as traffic management, air quality management, public safety solutions, smart parking, smart lightning and smart waste collection (Fig. 5). They mentioned that IoT is working hard to tackle these challenging issues. The need for improved smart city infrastructure with growing urbanization has opened the doors for entrepreneurs in the field of smart city technologies. The authors concluded that IoT enabled technology is very important for the development of sustainable smart cities.

Another important issue of IoT that requires attention and a lot of research is security and privacy. Weber [14] focused on these issues and suggested that a private organization availing IoT must incorporate data authentication, access control, resilience to attacks and client privacy into their business activities that would be an additional advantage.

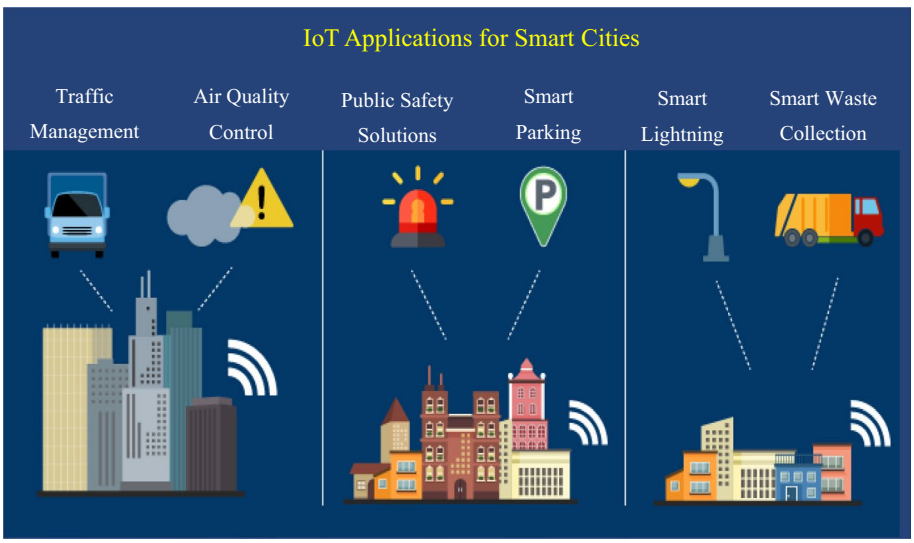

Fig. 5 Potential IoT application areas for smart cities

Weber suggested that in order to define global security and privacy issues, IoT developers must take into account the geographical limitations of the different countries. A generic framework needs to be designed to fit the global needs in terms of privacy and security. It is highly recommended to investigate and recognize the issues and challenges in privacy and security before developing the full fledge working IoT framework.

Later, Heer et al. [15] came up with a security issue in IP based IoT system. They mentioned that internet is backbone for the communication among devices that takes place in an IoT system. Therefore, security issues in IP based IoT systems are an important concern. In addition, security architecture should be designed considering the life cycle and capabilities of any object in the IoT system. It also includes the involvement of the trusted third party and the security protocols. The security architecture with scalability potential to serve the small-scale to large-scale things in IoT is highly desirable. The study pointed out that IoT gave rise to a new way of communication among several things across the network therefore traditional end to end internet protocol are not able to provide required support to this communication. Therefore, new protocols must be designed considering the translations at the gateways to ensure end-to-end security. Moreover, all the layers responsible for communication has their own security issues and requirements. Therefore, satisfying the requirements for one particular layers will leave the system into a vulnerable state and security should be ensured for all the layers.

Authentication and access control is another issue in IoT that needs promising solutions to strengthen the security. Liu et al. [16] brought up a solution to handle authentication and access control. Authentication is very important to verify the communicating parties to prevent the loss of confidential information. Liu et al. [16] provided an authentication scheme based on Elliptic Curve Cryptosystem and verified it on different security threats i.e. eavesdropping, man-in-the-middle attack, key control and replay attack. They claimed that there proposed schemes are able to provide better authentication and access control in IoT based communication. Later, Kothmayr et al. [17] proposed a two-way authentication scheme based of datagram transport layer security (DTLS) for IoT. The attackers over the internet are always active to steal the secured information. The proposed approach are able to provide message security, integrity, authenticity and confidentiality, memory overhead and end-to-end latency in the IoT based communication network.

Li et al. [18] proposed a dynamic approach for data centric IoT applications with respect to cloud platforms. The need of an appropriate device, software configuration and infrastructure requires efficient solutions to support massive amount of IoT applications that are running on cloud platforms. IoT developers and researchers are actively engaged in developing solutions considering both massive platforms and heterogeneous nature of IoT objects and devices. Olivier et al. [19] explained the concept of software defined networking (SDN) based architecture that performs well even if a well-defined architecture is not available. They proposed that SDN based security architecture is more flexible and efficient for IoT.

Luk et al. [20] stated that the main task of a secure sensor network (SSN) is to provide data privacy, protection from replay attacks and authentication. They discussed two popular SSN services namely TinySec [21] and ZigBee [22]. They mentioned that although both the SSN services are efficient and reliable, however, ZigBee is

comparatively provides higher security but consumes high energy whereas TinySec consumes low energy but not as highly secured as ZigBee. They proposed another architecture MiniSec to support high security and low energy consumption and demonstrated its performance for the Telos platform. Yan et al. [23] stated that trust management is an important issue in IoT. Trust management helps people to understand and trust IoT services and applications without worrying about uncertainty issues and risks [24]. They investigated different issues in trust management and discussed its importance with respect to IoT developers and users.

Noura et al. [25] stated the importance of interoperability in IoT as it allows integration of devices, services from different heterogeneous platforms to provide the efficient and reliable service. Several other studies focused on the importance of interoperability and discussed several challenges that interoperability issue is facing in IoT [26–28]. Kim et al. [29] addressed the issue of climate change and proposed an IoT based ecological monitoring system. They mentioned that existing approaches are time consuming and required a lot of human intervention. Also, a routine visit is required to collect the information from the sensors installed at the site under investigation. Also, some information remained missing which leads to not highly accurate analysis. Therefore, IoT based framework is able to solve this problem and can provide high accuracy in analysis and prediction. Later, Wang et al. [30] shows their concern for domestic waste water treatment. They discussed several deficiencies in the process of waste water treatment and dynamic monitoring system and suggested effective solutions based on IoT. They stated that IoT can be very effective in the waste water treatment and process monitoring.

Agriculture is one of the important domain around the world. Agriculture depends on several factors i.e. geographical, ecological etc. Qiu et al. [31] stated that technology that is being used for ecosystem control is immature with low intelligence level. They mentioned that it could be a good application area for IoT developers and researchers.

Qiu et al. [31] proposed an intelligent monitoring platform framework for facility agriculture ecosystem based on IoT that consists of four layer mechanism to manage the agriculture ecosystem. Each layer is responsible for specific task and together the framework is able to achieve a better ecosystem with reduced human intervention.

Another important concern around the world is climate change due to global warming. Fang et al. [32] introduced an integrated information system (IIS) that integrates IoT, geo-informatics, cloud computing, global positioning system (GPS), geographical information system (GIS) and e-science in order to provide an effective environmental monitoring and control system. They mentioned that the proposed IIS provides improved data collection, analysis and decision making for climate control. Air pollution is another important concern worldwide. Various tools and techniques are available to air quality measures and control. Cheng et al. [33] proposed AirCloud which is a cloud based air quality and monitoring system. They deployed AirCloud and evaluated its performance using 5 months data for the continuous duration of 2 months.

Temglit et al. [34] considered Quality of Service (QoS) as an important challenge and a complex task in evaluation and selection of IoT devices, protocols and services. QoS is very important criteria to attract and gain trust of users towards IoT services and devices. They came up with an interesting distributed QoS selection approach. This approach was based on distributed constraint optimization problem and multi-agent

Table 1 Comparative illustration of specific research studies on evaluation factors

Research	Major directions of study	Comparison based on evaluation factors				
		RT	RL	AV	CT	EC
Zhou et al. [3]	Security and privacy	–	x	–	–	x
Sfar et al. [4]	Architecture, security and privacy	x	–	x	x	–
Gaona-Garcia et al. [6]	Architecture, security and privacy	–	–	x		x
Behrendt [7]	Smart city, transport and healthcare	–	x	–	x	x
Zanella et al. [9]	Smart city, transport and healthcare	x	–	x	–	–
Khajenasiri et al. [10]	Environment, power and energy	x	–	x	x	x
Alavi et al. [13]	Smart city, transport and healthcare	–	x	–	x	
R.H. Weber [14]	Security and privacy	–	x	x	–	x
Heer et al. [15]	Security and privacy		x	–	–	x
Liu et al. [16]	Authentication and identification	x	x	–	x	–
Kothmayr et al. [17]	Security and privacy	–	x	–	–	–
Li et al. [18]	Security and privacy, management and control	–	x	x	x	–
Luk et al. [20]	Security and privacy, architecture	x	x	–	–	–
Sebastian and Ray [38]	Smart city, transport and healthcare, architecture	x	–	x		x
Yan et al. [23]	Authentication and identification, QoS	x	–	–	–	x
Dierks and Allen [44]	Standardization	x	–	x	–	–
Pei et al. [45]	Standardization, authentication and identification	–	x	–	–	x
Roman et al. [46]	Security and privacy	x		x	–	–
Noura et al. [25]	Interoperability	–	x		x	
Palattella et al. [27]	Interoperability, reliability, scalability	x	–	x	–	x
Yan et al. [23]	QoS, management and control, authentication and identification	–	x	–	x	–
Pereira and Aguiar [28]	Interoperability, QoS, scalability	x	–	x	–	x
Clausen et al. [66]	Data processing, reliability	–	x	x	x	–
Bao et al. [24]	Scalability, security and privacy	x	x	x	–	–
Li et al. [67]	Security and privacy, reliability	–	x		–	–
Zhang [68]	Security and privacy, data processing	–	x	x	–	
Qiu et al. [31]	Agriculture, environmental	x	x	–	–	x
Fang et al. [32]	Environmental	x	x	x	–	–
Montori et al. [69]	Interoperability, reliability	x	x	x	–	x
Distefano et al. [70]	Interoperability, scalability	x	–	–	–	x
Temglit et al. [34]	QoS, reliability	–	x	x	–	–
Talavera et al. [35]	Agriculture, industrial, environmental	x	–	–	x	x

RT response time, *RL* reliability, *AV* availability, *CT* cost, *EC* energy consumption

paradigm. Further, the approach was evaluated based on several experiments under realistic distributed environments. Another important aspect of IoT is its applicability to the environmental and agriculture standards. Talavera et al. [35] focused in this direction and presented the fundamental efforts of IoT for agro-industrial and environmental aspects in a survey study. They mentioned that the efforts of IoT in these areas are noticeable. IoT is strengthening the current technology and benefiting the farmers and society. Jara et al. [36] discussed the importance of IoT based monitoring of patients health. They suggested that IoT devices and sensors with the help of internet can assist health monitoring of patients. They also proposed a framework and protocol to achieve their objective. Table 1 provides a summary of the important studies and the direction of research with a comparison of studies on certain evaluation parameters.

IoT architecture and technologies

The IoT architecture consists of five important layers that defines all the functionalities of IoT systems. These layers are perception layer, network layer, middleware layer, application layer, business layer. At the bottom of IoT architecture, perception layer exists that consists of physical devices i.e. sensors, RFID chips, barcodes etc. and other physical objects connected in IoT network. These devices collects information in order to deliver it to the network layer. Network layer works as a transmission medium to deliver the information from perception layer to the information processing system. This transmission of information may use any wired/wireless medium along with 3G/4G, Wi-Fi, Bluetooth etc. Next level layer is known as middleware layer. The main task of this layer is to process the information received from the network layer and make decisions based on the results achieved from ubiquitous computing. Next, this processed information is used by application layer for global device management. On the top of the architecture, there is a business layer which control the overall IoT system, its applications and services. The business layer visualizes the information and statistics received from the application layer and further used this knowledge to plan future targets and strategies. Furthermore, the IoT architectures can be modified according to the need and application domain [19, 20, 37]. Besides layered framework, IoT system consists of several functional blocks that supports various IoT activities such as sensing mechanism, authentication and identification, control and management [38]. Figure 6 illustrates such functional blocks of IoT architecture.

There are several important functional blocks responsible for I/O operations, connectivity issues, processing, audio/video monitoring and storage management. All these functional block together incorporates an efficient IoT system which are important for optimum performance. Although, there are several reference architectures proposed with the technical specifications, but these are still far from the standard architecture that is suitable for global IoT [39]. Therefore, a suitable architecture is still needsvk to be designed that could satisfy the global IoT needs. The generic working structure of IoT system is shown in Fig. 7. Figure 7 shows a dependency of IoT on particular application parameters. IoT gateways have an important role in IoT communication as it allows connectivity between IoT servers and IoT devices related to several applications [40].

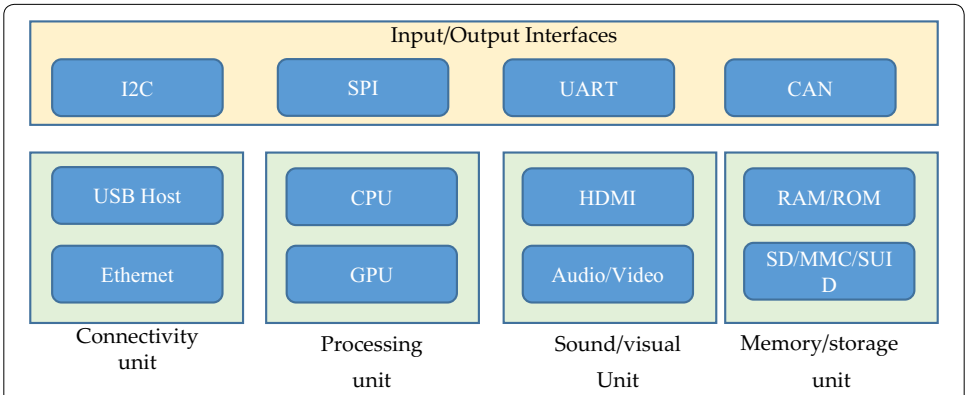

Fig. 6 A generic function module of IoT system

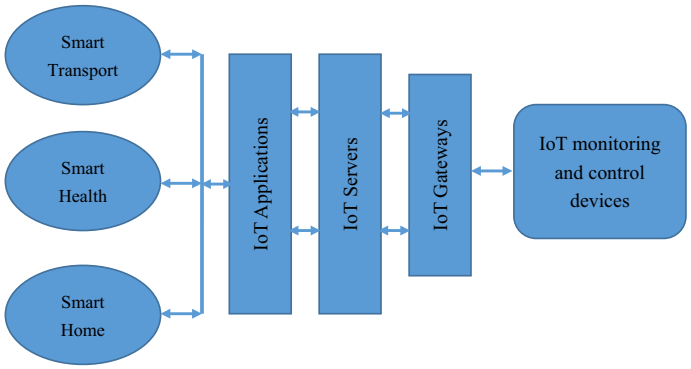

Fig. 7 Working structure of IoT

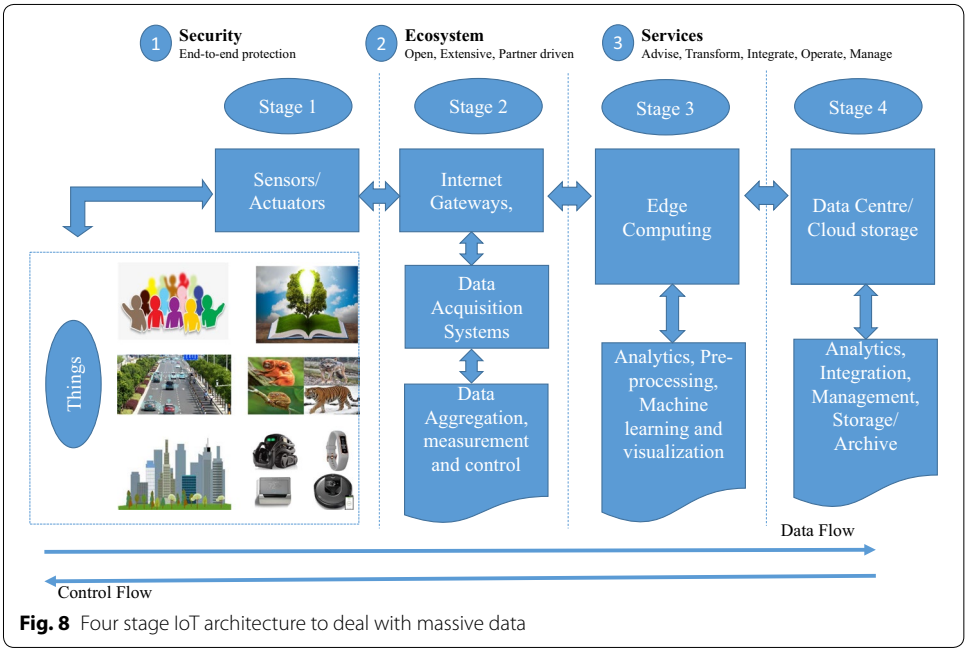

Fig. 8 Four stage IoT architecture to deal with massive data

Scalability, modularity, interoperability and openness are the key design issues for an efficient IoT architecture in a heterogenous environment. The IoT architecture must be designed with an objective to fulfil the requirements of cross domain interactions, multi-system integration with the potential of simple and scalable management functionalities, big data analytics and storage, and user friendly applications. Also, the architecture should be able to scaleup the functionality and add some intelligence and automation among the IoT devices in the system.

Moreover, increasing amount of massive data being generated through the communication between IoT sensors and devices is a new challenge. Therefore, an efficient architecture is required to deal with massive amount of streaming data in IoT system. Two popular IoT system architectures are cloud and fog/edge computing that supports with the handling, monitoring and analysis of huge amount of data in IoT systems. Therefore, a modern IoT architecture can be defined as a 4 stage architecture as shown in Fig. 8.

In stage 1 of the architecture, sensors and actuators plays an important role. Real world is comprised of environment, humans, animals, electronic gadgets, smart vehicles, and buildings etc. Sensors detect the signals and data flow from these real world entities and transforms into data which could further be used for analysis. Moreover, actuators is able to intervene the reality i.e. to control the temperature of the room, to slow down the vehicle speed, to turn off the music and light etc. Therefore, stage 1 assist in collecting data from real world which could be useful for further analysis. Stage 2 is responsible to collaborate with sensors and actuators along with gateways and data acquisition systems. In this stage, massive amount of data generated in stage 1 is aggregated and optimized in a structured way suitable for processing. Once the massive amount of data is aggregated and structured then it is ready to be passed to stage 3 which is edge computing. Edge computing can be defined as an open architecture in distributed fashion which allows use of IoT technologies and massive computing power from different locations worldwide. It is very powerful approach for streaming data processing and thus suitable for IoT systems. In stage 3, edge computing technologies deals with massive amount of data and provides various functionalities such as visualization, integration of data from other sources, analysis using machine learning methods etc. The last stage comprises of several important activities such as in depth processing and analysis, sending feedback to improve the precision and accuracy of the entire system. Everything at this stage will be performed on cloud server or data centre. Big data framework such as Hadoop and Spark may be utilized to handle this large streaming data and machine learning approaches can be used to develop better prediction models which could help in a more accurate and reliable IoT system to meet the demand of present time.

Major key issues and challenges of IoT

The involvement of IoT based systems in all aspects of human lives and various technologies involved in data transfer between embedded devices made it complex and gave rise to several issues and challenges. These issues are also a challenge for the IoT developers in the advanced smart tech society. As technology is growing, challenges and need for advanced IoT system is also growing. Therefore, IoT developers need to think of new issues arising and should provide solutions for them.

Security and privacy issues

One of the most important and challenging issues in the IoT is the security and privacy due to several threats, cyber attacks, risks and vulnerabilities [41]. The issues that give rise to device level privacy are insufficient authorization and authentication, insecure software, firmware, web interface and poor transport layer encryption [42]. Security and privacy issues are very important parameters to develop confidence in IoT Systems with respect to various aspects [43]. Security mechanisms must be embedded at every layer of IoT architecture to prevent security threats and attacks [23]. Several protocols are developed and efficiently deployed on every layer of communication channel to ensure the security and privacy in IoT based systems [44, 45]. Secure Socket Layer (SSL) and Datagram Transport Layer Security (DTLS) are one of the cryptographic protocols that are implemented between transport and application layer to provide security solutions in various IoT systems [44]. However, some IoT applications require different methods

to ensure the security in communication between IoT devices. Besides this, if communication takes place using wireless technologies within the IoT system, it becomes more vulnerable to security risks. Therefore, certain methods should be deployed to detect malicious actions and for self healing or recovery. Privacy on the other hand is another important concern which allows users to feel secure and comfortable while using IoT solutions. Therefore, it is required to maintain the authorization and authentication over a secure network to establish the communication between trusted parties [46]. Another issue is the different privacy policies for different objects communicating within the IoT system. Therefore, each object should be able to verify the privacy policies of other objects in IoT system before transmitting the data.

Interoperability/standard issues

Interoperability is the feasibility to exchange the information among different IoT devices and systems. This exchange of information does not rely on the deployed software and hardware. The interoperability issue arises due to the heterogeneous nature of different technology and solutions used for IoT development. The four interoperability levels are technical, semantic, syntactic and organizational [47]. Various functionalities are being provided by IoT systems to improve the interoperability that ensures communication between different objects in a heterogeneous environment. Additionally, it is possible to merge different IoT platforms based on their functionalities to provide various solutions for IoT users [48]. Considering interoperability an important issue, researchers approved several solutions that are also know as interoperability handling approaches [49]. These solutions could be adapaters/gateways based, virtual networks/overlay based, service oriented architecture based etc. Although interoperability handling approaches ease some pressure on IoT systems but there are still certain challenges remain with interoperability that could be a scope for future studies [25].

Ethics, law and regulatory rights

Another issue for IoT developers is the ethics, law and regulatory rights. There are certain rules and regulations to maintain the standard, moral values and to prevent the people from violating them. Ethics and law are very similar term with the only difference is that ethics are standards that people believes and laws are certain restrictions decided by the government. However, both ethics and laws are designed to maintain the standard, quality and prevent people from illegal use. With the development of IoT, several real life problems are solved but it has also given rise to critical ethical and legal challenges [50]. Data security, privacy protection, trust and safety, data usability are some of those challenges. It has also been observed that majority of IoT users are supporting government norms and regulations with respect to data protection, privacy and safety due to the lack of trust in IoT devices. Therefore, this issue must be taken into consideration to maintain and improve the trust among people for the use of IoT devices and systems.

Scalability, availability and reliability

A system is scalable if it is possible to add new services, equipments and devices without degrading its performance. The main issue with IoT is to support a large number of devices with different memory, processing, storage power and bandwidth [28]. Another

important issue that must be taken into consideration is the availability. Scalability and availability both should be deployed together in the layered framework of IoT. A great example of scalability is cloud based IoT systems which provide sufficient support to scale the IoT network by adding up new devices, storage and processing power as required.

However, this global distributed IoT network gives rise to a new research paradigm to develop a smooth IoT framework that satisfy global needs [51]. Another key challenge is the availability of resources to the authentic objects regardless of their location and time of the requirement. In a distributed fashion, several small IoT networks are timely attached to the global IoT platforms to utilize their resources and services. Therefore, availability is an important concern [52]. Due to the use of different data transmission channels i.e. satellite communication, some services and availability of resources may be interrupted. Therefore, an independent and reliable data transmission channel is required for uninterrupted availability of resources and services.

Quality of Service (QoS)

Quality of Service (QoS) is another important factor for IoT. QoS can be defined as a measure to evaluate the quality, efficiency and performance of IoT devices, systems and architecture [34]. The important and required QoS metrics for IoT applications are reliability, cost, energy consumption, security, availability and service time [53]. A smarter IoT ecosystem must fulfill the requirements of QoS standards. Also, to ensure the reliability of any IoT service and device, its QoS metrics must be defined first. Further, users may also be able to specifiy their needs and requirements accordingly. Several approaches can be deployed for QoS assessment, however as mentioned by White et al. [54] there is a trade-off between quality factors and approaches. Therefore, good quality models must be deployed to overcome this trade-off. There are certain good quality models available in literature such as ISO/IEC25010 [55] and OASIS-WSQM [56] which can be used to evaluate the approaches used for QoS assessment. These models provides a wide range of quality factors that is quite sufficient for QoS assessment for IoT services. Table 2 summarizes the different studies with respect to IoT key challenges and issues discussed above.

Major IoT applications

Emerging economy, environmental and health-care

IoT is completely devoted to provide emerging public and financial benefits and development to the society and people. This includes a wide range of public facilities i.e. economic development, water quality maintenance, well-being, industrialization etc. Overall, IoT is working hard to accomplish the social, health and economic goals of United Nations advancement step. Environmental sustainability is another important concern. IoT developers must be concerned about environmental impact of the IoT systems and devices to overcome the negative impact [48]. Energy consumption by IoT devices is one of the challenges related to environmental impact. Energy consumption is increasing at a high rate due to internet enabled services and edge cutting devices. This area needs research for the development of high quality materials in order to create new IoT devices with lower energy consumption rate. Also, green technologies can be

Table 2 A summary of studies with respect to IoT key challenges and applications

IoT key issues	References	Specific concepts covered
Interoperability	[25–28, 47–49, 71–75]	General issues, IoT platforms and architectures, technical and semantic interoperability
Security and privacy	[1–6, 14, 15, 17–20, 24, 46, 76]	Security and privacy issues, definition and design of secure IoT networks and architecture
Management and control	[12, 18, 23, 26, 43, 71, 73, 77–80]	IoT layer management and control, device, network, application, data and trust management and control
Architecture	[4, 6, 19, 20, 38, 74, 75, 81–85]	Hardware, cloud centric, SOA, process architectures and conceptual models, application frameworks
Quality of Service	[23, 26, 28, 34, 41, 53, 86–94]	Data traffic load, protocols for all layers in IoT architecture, QoS and QoE routine check
Authentication and identification	[12, 16, 17, 23, 45, 50, 95–97]	Addressing issues and solutions, IoT integrations with internet protocols (IPv6), authentication and identification issues
Environment, power and energy	[10, 29–33, 37, 67, 68, 85, 98–102]	Involvement of green technology in IoT, design of low power consumption devices and chips, pollution control and management
Smart city, healthcare and transportation	[7, 9, 10, 13, 38, 58, 69, 70, 103–113]	Smart traffic management and control, smart devices for healthcare management, smart vehicles, energy management
Data processing and storage	[26, 41, 43, 66, 87, 114]	Data analysis, visualization, integration issues and solutions
Reliability	[18, 27, 43, 52, 66, 72, 101, 115–121]	Connectivity, mobility and routing issues, reliability of infrastructure and applications
Scalability	[24, 27, 28, 41, 43, 51, 115]	Scaling issues on large platforms and geographical locations, potential discovery services
Standardization	[12, 43–45, 99, 101, 114, 122]	IoT definition, protocols design, architecture standardization, vision and framework design

adopted to create efficient energy efficient devices for future use. It is not only environmental friendly but also advantageous for human health. Researchers and engineers are engaged in developing highly efficient IoT devices to monitor several health issues such as diabetes, obesity or depression [57]. Several issues related to environment, energy and healthcare are considered by several studies.

Smart city, transport and vehicles

IoT is transforming the traditional civil structure of the society into high tech structure with the concept of smart city, smart home and smart vehicles and transport. Rapid improvements are being done with the help of supporting technologies such as machine learning, natural language processing to understand the need and use of technology at home [58]. Various technologies such as cloud server technology, wireless sensor networks that must be used with IoT servers to provide an efficient smart city. Another important issue is to think about environmental aspect of smart city. Therefore, energy

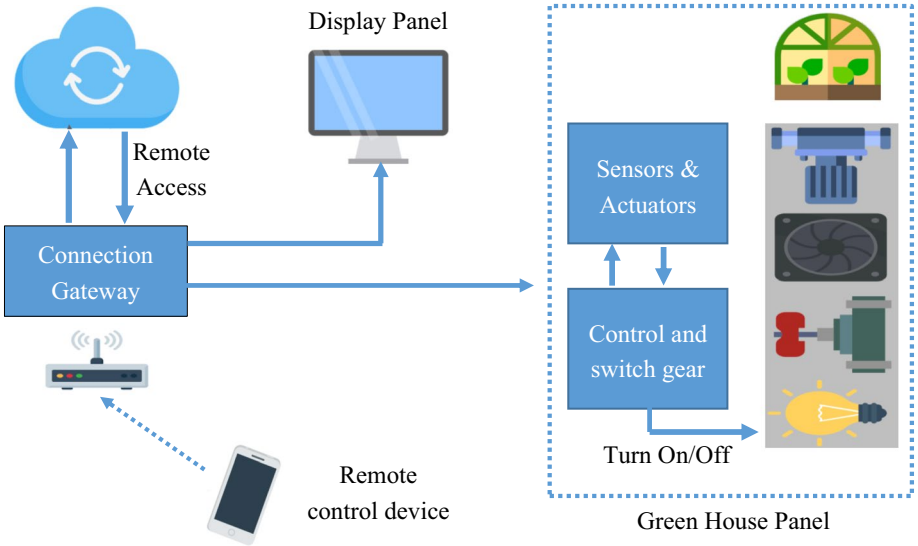

Fig. 9 A working structure of IoT system in agriculture production

efficient technologies and Green technologies should also be considered for the design and planning of smart city infrastructure. Further, smart devices which are being incorporated into newly launched vehicles are able to detect traffic congestions on the road and thus can suggest an optimum alternate route to the driver. This can help to lower down the congestion in the city. Furthermore, smart devices with optimum cost should be designed to be incorporated in all range vehicles to monitor the activity of engine. IoT is also very effective in maintaining the vehicle's health. Self driving cars have the potential to communicate with other self driving vehicles by the means of intelligent sensors. This would make the traffic flow smoother than human-driven cars who used to drive in a stop and go manner. This procedure will take time to be implemented all over the world. Till the time, IoT devices can help by sensing traffic congestion ahead and can take appropriate actions. Therefore, a transport manufacturing company should incorporate IoT devices into their manufactured vehicles to provide its advantage to the society.

Agriculture and industry automation

The world's growing population is estimated to reach approximate 10 billion by 2050. Agriculture plays an important role in our lives. In order to feed such a massive population, we need to advance the current agriculture approaches. Therefore, there is a need to combine agriculture with technology so that the production can be improved in an efficient way. Greenhouse technology is one of the possible approaches in this direction. It provides a way to control the environmental parameters in order to improve the production. However, manual control of this technology is less effective, need manual efforts and cost, and results in energy loss and less production. With the advancement of IoT, smart devices and sensors makes it easier to control the climate inside the chamber and monitor the process which results in energy saving and improved production (Fig. 9). Automatization of industries is another advantage of IoT. IoT has been providing

game changing solutions for factory digitalization, inventory management, quality control, logistics and supply chain optimization and management.

Importance of big data analytics in IoT

An IoT system comprises of a huge number of devices and sensors that communicates with each other. With the extensive growth and expansion of IoT network, the number of these sensors and devices are increasing rapidly. These devices communicate with each other and transfer a massive amount of data over internet. This data is very huge and streaming every second and thus qualified to be called as big data. Continuous expansion of IoT based networks gives rise to complex issue such as management and collection of data, storage and processing and analytics. IoT big data framework for smart buildings is very useful to deal with several issues of smart buildings such as managing oxygen level, to measure the smoke/hazardous gases and luminosity [59]. Such framework is capable to collect the data from the sensors installed in the buildings and performs data analytics for decision making. Moreover, industrial production can be improved using an IoT based cyber physical system that is equipped with an information analysis and knowledge acquisition techniques [60]. Traffic congestion is an important issue with smart cities. The real time traffic information can be collected through IoT devices and sensors installed in traffic signals and this information can be analyzed in an IoT based traffic management system [61]. In healthcare analysis, the IoT sensors used with patients generate a lot of information about the health condition of patients every second. This large amount of information needs to be integrated at one database and must be processed in real time to take quick decision with high accuracy and big data technology is the best solution for this job [62]. IoT along with big data analytics can also help to transform the traditional approaches used in manufacturing industries into the modern one [63]. The sensing devices generates information which can be analyzed using big data approaches and may help in various decision making tasks. Furthermore, use of cloud computing and analytics can benefit the energy development and conservation with reduced cost and customer satisfaction [64]. IoT devices generate a huge amount of streaming data which needs to be stored effectively and needs further analysis for decision making in real time. Deep learning is very effective to deal with such a large information and can provide results with high accuracy [65]. Therefore, IoT, Big data analytics and Deep learning together is very important to develop a high tech society.

Conclusions

Recent advancements in IoT have drawn attention of researchers and developers worldwide. IoT developers and researchers are working together to extend the technology on large scale and to benefit the society to the highest possible level. However, improvements are possible only if we consider the various issues and shortcomings in the present technical approaches. In this survey article, we presented several issues and challenges that IoT developer must take into account to develop an improved model. Also, important application areas of IoT is also discussed where IoT developers and researchers are engaged. As IoT is not only providing services but also

generates a huge amount of data. Hence, the importance of big data analytics is also discussed which can provide accurate decisions that could be utilized to develop an improved IoT system.

Abbreviations
IoT: Internet of Things; QoS: Quality of Service; WoT: Web of Things; CoT: Cloud of Things; SHS: Smart Home System; SHSS: Smart Health Sensing System.

Acknowledgements
This work was financially supported by the Ministry of Education and Science of Russian Federation (government order 2.7905.2017/8.9).

Authors' contributions
SK and PT prepared the draft and Idea. SK wrote the manuscript. MZ prepared the tables, references and checked the English. All authors read and approved the final manuscript.

Funding
The research received no external funding.

Availability of data and materials
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Author details
[1] Department of Computer Science, South Ural State University, Chelyabinsk, Russian Federation. [2] Department of Information Engineering, University of Padova, Padua, Italy.

Received: 24 July 2019 Accepted: 10 November 2019
Published online: 09 December 2019

References

1. Sfar AR, Zied C, Challal Y. A systematic and cognitive vision for IoT security: a case study of military live simulation and security challenges. In: Proc. 2017 international conference on smart, monitored and controlled cities (SM2C), Sfax, Tunisia, 17–19 Feb. 2017. https://doi.org/10.1109/sm2c.2017.8071828.
2. Gatsis K, Pappas GJ. Wireless control for the IoT: power spectrum and security challenges. In: Proc. 2017 IEEE/ACM second international conference on internet-of-things design and implementation (IoTDI), Pittsburg, PA, USA, 18–21 April 2017. INSPEC Accession Number: 16964293.
3. Zhou J, Cap Z, Dong X, Vasilakos AV. Security and privacy for cloud-based IoT: challenges. IEEE Commun Mag. 2017;55(1):26–33. https://doi.org/10.1109/MCOM.2017.1600363CM.
4. Sfar AR, Natalizio E, Challal Y, Chtourou Z. A roadmap for security challenges in the internet of things. Digit Commun Netw. 2018;4(1):118–37.
5. Minoli D, Sohraby K, Kouns J. IoT security (IoTSec) considerations, requirements, and architectures. In: Proc. 14th IEEE annual consumer communications & networking conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017. https://doi.org/10.1109/ccnc.2017.7983271.
6. Gaona-Garcia P, Montenegro-Marin CE, Prieto JD, Nieto YV. Analysis of security mechanisms based on clusters IoT environments. Int J Interact Multimed Artif Intell. 2017;4(3):55–60.
7. Behrendt F. Cycling the smart and sustainable city: analyzing EC policy documents on internet of things, mobility and transport, and smart cities. Sustainability. 2019;11(3):763.
8. IoT application areas. https://iot-analytics.com/top-10-iot-project-application-areas-q3-2016/. Accessed 05 Apr 2019.
9. Zanella A, Bui N, Castellani A, Vangelista L, Zorgi M. Internet of things for smart cities. IEEE IoT-J. 2014;1(1):22–32.
10. Khajenasiri I, Estebsari A, Verhelst M, Gielen G. A review on internet of things for intelligent energy control in buildings for smart city applications. Energy Procedia. 2017;111:770–9.
11. Internet of Things. http://www.ti.com/technologies/internet-of-things/overview.html. Accessed 01 Apr 2019.
12. Liu T, Yuan R, Chang H. Research on the internet of things in the automotive industry. In: ICMeCG 2012 international conference on management of e-commerce and e-Government, Beijing, China. 20–21 Oct 2012. p. 230–3.
13. Alavi AH, Jiao P, Buttlar WG, Lajnef N. Internet of things-enabled smart cities: state-of-the-art and future trends. Measurement. 2018;129:589–606.
14. Weber RH. Internet of things-new security and privacy challenges. Comput Law Secur Rev. 2010;26(1):23–30.
15. Heer T, Garcia-Morchon O, Hummen R, Keoh SL, Kumar SS, Wehrle K. Security challenges in the IP based internet of things. Wirel Pers Commun. 2011;61(3):527–42.
16. Liu J, Xiao Y, Philip-Chen CL. Authentication and access control in the internet of things. In: 32nd international conference on distributed computing systems workshops, Macau, China. IEEE xplore; 2012. https://doi.org/10.1109/icdcsw.2012.23 .
17. Kothmayr T, Schmitt C, Hu W, Brunig M, Carle G. DTLS based security and two-way authentication for the internet of things. Ad Hoc Netw. 2013;11:2710–23.

18. Li Y, et al. IoT-CANE: a unified knowledge management system for data centric internet of things application systems. J Parallel Distrib Comput. 2019;131:161–72.
19. Olivier F, Carlos G, Florent N. New security architecture for IoT network. In: International workshop on big data and data mining challenges on IoT and pervasive systems (BigD2M 2015), procedia computer science, vol. 52; 2015. p. 1028–33.
20. Luk M, Mezzour G, Perrig A, Gligor V. MiniSec: a secure sensor netowrk communication architecture. In: Proc: 6th international symposium on information processing in sensor networks, Cambridge, MA, USA, 25–27 April 2007.
21. Karlof C, Sastry N, Wagner D. TinySec: a link layer security architecture for wireless sensor networks. In: Proceedings of the second ACM conference on embedded networked sensor systems (SenSys 2004), November 2004.
22. ZigBee Alliance. Zigbee specification. Technical Report Document 053474r06, Version 1.0, ZigBee Alliance, June 2005.
23. Yan Z, Zhang P, Vasilakos AV. A survey on trust management for internet of things. J Netw Comput Appl. 2014;42:120–34.
24. Bao F, Chen I-R, Guo J. Scalable, adaptive and survivable trust management for community of interest based internet of things systems. In: Proc. IEEE 11th international symposium on autonomous decentralized systems (ISADS); 2013. p. 1–7.
25. Noura M, Atiquazzaman M, Gaedke M. Interoperability in internet of things: taxonomies and open challenges. Mob Netw Appl. 2019;24(3):796–809.
26. 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(June):2347–76.
27. Palattella MR, Dohler M, Grieco A, Rizzo G, Torsner J, Engel T, Ladid L. Internet of things in the 5G era: enablers, architecture and business models. IEEE J Sel Areas Commun. 2016;34(3):510–27.
28. Pereira C, Aguiar A. Towards efficient mobile M2M communications: survey and open challenges. Sensors. 2014;14(10):19582–608.
29. Kim NS, Lee K, Ryu JH. Study on IoT based wild vegetation community ecological monitoring system. In: Proc. 2015 7th international conference on ubiquitous and future networks, Sapporo, Japan, 7–10 July 2015. IEEE.
30. Wang JY, Cao Y, Yu GP, Yuan M. Research on applications of IoT in domestic waste treatment and disposal. In: Proc. 11th World congress on intelligent control and automation, Shenyang, China, 2014. IEEE.
31. Qiu T, Xiao H, Zhou P. Framework and case studies of intelligent monitoring platform in facility agriculture ecosystem. In: Proc. 2013 second international conference on agro-geoinformatics (agro-geoinformatics), Fairfax, VA, USA, 12–16 Aug 2013. IEEE.
32. Fang S, et al. An integrated system for regional environmental monitoring and management based on internet of things. IEEE Trans Ind Inf. 2014;10(2):1596–605.
33. Cheng Y, et al. AirCloud: a cloud based air-quality monitoring system for everyone. In: Proceedings of the 12th ACM conference on embedded network sensor systems, ACM, Memphis, Tennessee, 03–06 Nov 2014. p. 251–65.
34. Temglit N, Chibani A, Djouani K, Nacer MA. A distributed agent-based approach for optimal QoS selection in web of object choreography. IEEE Syst J. 2018;12(2):1655–66.
35. Talavera JM, et al. Review of IoT applications in agro-industrial and environmental fields. Comput Electron Agric. 2017;142(7):283–97.
36. Jara AJ, Zamora-Izquierdo MA, Skarmeta AF. Interconnection framework for mHealth and remote monitoring based in the internet of things. IEEE J Sel Areas Commun. 2013;31(9):47–65.
37. 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):1645–60.
38. Sebastian S, Ray PP. Development of IoT invasive architecture for complying with health of home. In: Proc: I3CS, Shillong; 2015. p. 79–83.
39. Nicolescu R, Huth M, Radanliev P, Roure DD. Mapping the values of IoT. J Inf Technol. 2018;33(4):345–60.
40. Hu P, Ning H, Qiu T, Xu Y, Luo X, Sangaiah AK. A unified face identification and resolutions scheme using cloud computing in internet of things. Future Gener Comput Syst. 2018;81:582–92.
41. Babovic ZB, Protic V, Milutinovic V. Web performance evaluation for internet of things applications. IEEE Access. 2016;4:6974–92.
42. Internet of Things research study: Hewlett Packard Enterprise Report. 2015. http://www8.hp.com/us/en/hp-news/press-release.html?id=1909050#.WPoNH6KxWUk.
43. Xu LD, He W, Li S. Internet of things in industries: a survey. IEEE Trans Ind Inf. 2014;10(4):2233–43.
44. Dierks T, Allen C. The TLS protocol version 1.0, IETF RFC, 2246; 1999. https://www.ietf.org/rfc/rfc2246.txt.
45. Pei M, Cook N, Yoo M, Atyeo A, Tschofenig H. The open trust protocol (OTrP). IETF 2016. https://tools.ietf.org/html/draft-pei-opentrustprotocol-00.
46. Roman R, Najera P, Lopez J. Securing the internet of things. Computer. 2011;44(9):51–8.
47. Van-der-Veer H, Wiles A. Achieving technical, interoperability-the ETSI approach, ETSI White Paper No. 3. 2008.http://www.etsi.org/images/files/ETSIWhitePapers/IOP%20whitepaper%20Edition%203%20final.pdf.
48. Colacovic A, Hadzialic M. Internet of things (IoT): a review of enabling technologies, challenges and open research issues. Comput Netw. 2018;144:17–39.
49. Noura M, Atiquazzaman M, Gaedke M. Interoperability in internet of things infrastructure: classification, challenges and future work. In: Third international conference, IoTaaS 2017, Taichung, Taiwan. 20–22 September 2017.
50. Tzafestad SG. Ethics and law in the internet of things world. Smart Cities. 2018;1(1):98–120.
51. Mosko M, Solis I, Uzun E, Wood C. CCNx 1.0 protocol architecture. A Xerox company, computing science laboratory PARC; 2017.
52. Wu Y, Li J, Stankovic J, Whitehouse K, Son S, Kapitanova K. Run time assurance of application-level requirements in wireless sensor networks. In: Proc. 9th ACM/IEEE international conference on information processing in sensor networks, Stockholm, Sweden, 21–16 April 2010. p. 197–208.
53. Huo L, Wang Z. Service composition instantiation based on cross-modified artificial Bee Colony algorithm. Chin Commun. 2016;13(10):233–44.

54. White G, Nallur V, Clarke S. Quality of service approaches in IoT: a systematic mapping. J Syst Softw. 2017;132:186–203.
55. ISO/IEC 25010—Systems and software engineering—systems and software quality requirements and evaluation (SQuaRE)—system and software quality models, Technical Report; 2010.
56. Oasis. Web services quality factors version 1.0. 2012. http://docs.oasis-open.org/wsqm/wsqf/v1.0/WS-Quality-Factors.pdf.
57. Fafoutis X, et al. A residential maintenance-free long-term activity monitoring system for healthcare applications. EURASIP J Wireless Commun Netw. 2016. https://doi.org/10.1186/s13638-016-0534-3.
58. Park E, Pobil AP, Kwon SJ. The role of internet of things (IoT) in smart cities: technology roadmap-oriented approaches. Sustainability. 2018;10:1388.
59. Bashir MR, Gill AQ. Towards an IoT big data analytics framework: smart buildings system. In: IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems; 2016. p. 1325–32.
60. Lee C, Yeung C, Cheng M. Research on IoT based cyber physical system for industrial big data analytics. In: 2015 IEEE international conference on industrial engineering and engineering management (IEEM). New York: IEEE; 2015. p. 1855–9.
61. Rizwan P, Suresh K, Babu MR. Real-time smart traffic management system for smart cities by using internet of things and big data. In: International conference on emerging techno-logical trends (ICETT). New York: IEEE; 2016. p. 1–7.
62. Vuppalapati C, Ilapakurti A, Kedari S. The role of big data in creating sense EHR, an integrated approach to create next generation mobile sensor and wear-able data driven electronic health record (EHR). In: 2016 IEEE second international conference on big data computing service and applications (BigDataService). New York: IEEE; 2016. p. 293–6.
63. Mourtzis D, Vlachou E, Milas N. Industrial big data as a result of IoT adoption in manufacturing. Procedia CIRP. 2016;55:290–5.
64. Ramakrishnan R, Gaur L. Smart electricity distribution in residential areas: Internet of things (IoT) based advanced metering infrastructure and cloud analytics. In: International Conference on internet of things and applications (IOTA). New York: IEEE; 2016. p. 46–51.
65. Mohammadi M, Al-Fuqaha A, Sorour S, Guizani M. Deep learning for IoT big data and streaming analytics: a survey. IEEE Commun Surv Tutor. 2018;20(4):2923–60.
66. Clausen T, Herberg U, Philipp M. A critical evaluation of the IPv6 routing protocol for low power and lossy networks (RPL). In: 2011 IEEE 7th international conference on wireless and mobile computing, networking and communications (WiMob), Wuhan, China, 10–12 Oct 2011.
67. Li H, Wang H, Yin W, Li Y, Qian Y, Hu F. Development of remote monitoring system for henhouse based on IoT technology. Future Internet. 2015;7(3):329–41.
68. Zhang L. An IoT system for environmental monitoring and protecting with heterogeneous communication networks. In: Proc. 2011 6th international ICST conference on communications and networking in China (CHINACOM), Harbin, China, 17–19 Aug 2011. IEEE.
69. Montori F, Bedogni L, Bononi L. A collaborative internet of things architecture for smart cities and environmental monitoring. IEEE Internet Things J. 2018;5(2):592–605.
70. Distefano S, Longo F, Scarpa M. QoS assessment of mobile crowd sensing services. J Grid Comput. 2015;13(4):629–50.
71. Stankovic JA. Research directions for the internet of things. IEEE Internet Things J. 2014;1(1):3–9.
72. Al-Fuqaha A, Khreishah A, Guizani M, Rayes A, Mohammadi M. Toward better horizontal integration among IoT services. IEEE Commun Mag. 2015;53(9):72–9.
73. Chen IR, Guo J, Bao F. Trust management for SOA-based IoT and its application to service composition. IEEE Trans Serv Comput. 2016;9(3):482–95.
74. Sarkar C, et al. DIAT: a scalable distributed architecture for IoT. IEEE Internet Things J. 2014;2(3):230–9.
75. Chen S, Xu H, Liu D, Hu B, Wang H. A vision of IoT: applications, challenges, and opportunities with China perspective. IEEE Internet Things J. 2014;1(4):349–59.
76. Kang K, Pang J, Xu LD, Ma L, Wang C. An interactive trust model for application market of the internet of things. IEEE Trans Ind Inf. 2014;10(2):1516–26.
77. Gupta A, Jha RK. A survey of 5G network: architecture and emerging technologies. IEEE Access. 2015;3:1206–32.
78. Vlacheas P, et al. Enabling smart cities through a cognitive management framework for the internet of things. IEEE Commun Mag. 2013;51(6):102–11.
79. Bizanis N, Kuipers FA. SDN and virtualization solutions for the internet of things: a survey. IEEE Access. 2016;4:5591–606.
80. Zeng X, et al. IOTSim: a simulator for analyzing IoT applications. J Syst Architect. 2017;72:93–107.
81. Fantacci R, Pecorella T, Viti R, Carlini C. A network architecture solutions for efficient IOT WSN backhauling: challenges and opportunities. IEEE Wirel Commun. 2014;21(4):113–9.
82. Kim M, Ahn H, Kim KP. Process-aware internet of things: a conceptual extension of the internet of things framework and architecture. KSII Trans Internet Inf Syst. 2016;10(8):4008–22.
83. Hsieh H-C, Chang K-D, Wang L-F, Chen J-L, Chao H-C. ScriptIoT: a script framework for and internet of things applications. IEEE Internet Things J. 2015;3(4):628–36.
84. Kiljander J, et al. Semantic interoperability architecture for pervasive computing and internet of things. IEEE Access. 2014;2:856–73.
85. Ye J, Chen B, Liu Q, Fang Y. A precision agriculture management system based on internet of things and WebGIS. In: Proc. 2013 21st international conference on geoinformatics, Kaifeng, China, 20–22 June 2013. IEEE.
86. Jara AJ, Martinez-Julia P, Skarmeta A. Light-weight multicast DNS and DNS-SD (lmDNS-SD): IPv6-based resource and service discovery for web of things. In: Proc. sixth international conference on innovative mobile and internet services in ubiquitous computing, Palermo, Italy, 4–6 July 2012.

87. Diaz M, Martin C, Rubio B. State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing. J Netw Comput Appl. 2016;67:99–117.
88. Lo A, Law YW, Jacobsson M. A cellular-centric service architecture for machine to machine (M2M) communications. IEEE Wirel Commun. 2013;20(5):143–51.
89. Kecskemeti G, Casale G, Jha DN, Lyon J, Ranjan R. Modeling and simulation challenges in internet of things. IEEE Cloud Comput. 2017;4(1):62–9.
90. Cuomo S, Somma VD, Sica F. An application of the one-factor HullWhite model in an IoT financial scenario. Sustain Cities Soc. 2018;38:18–20.
91. Liu J, et al. A cooperative evolution for QoS-driven IOT service composition. Autom J Control Meas Electron Comput Commun. 2013;54(4):438–47.
92. Huo Y, et al. Multi-objective service composition model based on cost-effective optimization. Appl Intell. 2017;48(3):651–69.
93. Han SN, Crespi N. Semantic service provisioning for smart objects: integrating IoT applications into the web. Future Gener Comput Syst. 2017;76:180–97.
94. Alodib M. QoS-aware approach to monitor violations of SLAs in the IoT. J Innov Digit Ecosyst. 2016;3(2):197–207.
95. Rizzardi A, Sicari S, Miorandi D, Coen-Porisini A. AUPS: an open source authenticated publish/subscribe system for internet of things. Inf Syst. 2016;62:29–41.
96. Fenye B, Ing-Ray C, Jia G. Scalable, adaptive and survivable trust management for community of interest based internet of things systems. In: Proc. IEEE eleventh international symposium on autonomous decentralized systems (ISADS), Mexico City, Mexico, 6–8 March 2013.
97. Tehrani MN, Uysal M, Yanikomeroglu H. Device to device communication in 5G cellular networks: challenges, solutions, and future directions. IEEE Commun Mag. 2014;52(5):86–92.
98. Zhu C, Leung VCM, Shu L, Ngai ECH. Green internet of things for smart world. IEEE Access. 2015;3:2151–62.
99. Adame T, Bel A, Bellalta B, Barcelo J, Oliver M. IEEE 802.11AH: the WiFi approach for M2M communications. IEEE Wirel Commun. 2014;21(6):144–52.
100. Shaikh FK, Zeadally S, Exposito E. Enabling technologies for green internet of things. IEEE Syst J. 2015;99:1–12.
101. Palattella MR, et al. Standardized protocol stack for the internet of (important) things. IEEE Commun Surv Tutor. 2012;15(3):1389–406.
102. Vatari S, Bakshi A, Thakur T. Green house by using IoT and cloud computing. In: Proc. 2016 IEEE international conference on recent trends in electronic, information & communication technology (RTEICT), Bangalore, India, 20–21 May 2016.
103. Chiang M, Zhang T. Fog and IoT: an overview of research opportunities. IEEE Internet Things J. 2016;3(6):854–64.
104. Elkhodr M, Shahrestani S, Cheung H. A smart home application based on the internet of things management platform. In: Proc. 2015 IEEE international conference on data science and data intensive systems, Sydney, Australia, 11–13 Dec 2015.
105. Talari S, et al. A review of smart cities based on the internet of things concept. Energies. 2017;10(4):421–43.
106. Burange AW, Misalkar HD. Review of internet of things in development of smart cities with data management & privacy. In: Proc. 2015 international conference on advances in computer engineering and applications, Ghaziabad, India, 19–20 March 2015.
107. Zia T, Liu P, Han W. Application-specific digital forensics investigative model in internet of things (IoT). In: Proc. 12th international conference on availability, reliability and security, Reggio Calabria, Italy; 2017.
108. Lingling H, Haifeng L, Xu X, Jian L. An intelligent vehicle monitoring system based on internet of things. In: Proc. 7th international conference on computational intelligence and security, Hainan, China, 3–4 Dec 2011. IEEE.
109. Duttagupta S, Kumar M, Ranjan R, Nambiar M. Performance prediction of IoT application: an experimental analysis. In: Proc. 6th international conference on the internet of things, Stuttgart, Germany, 07–09 Nov 2016. p. 43–51.
110. Chen S, Liu B, Chen X, Zhang Y, Huang G. Framework for adaptive computation offloading in IoT applications. In: Proc. 9th Asia-Pacific symposium on internetware, Shanghai, China, 23 Sep 2017. ACM.
111. Li Q, Dou R, Chen F, Nan G. A QoS-oriented web service composition approach based on multi-population genetic algorithm for internet of things. Int J Comput Intell Syst. 2014;7(Sup2):26–34.
112. Urbieta A, Gonzalez-Beltran A, Mokhtar SB, Hossain MA, Capra L. Adaptive and context-aware service composition for IoT-based smart cities. Future Gener Comput Syst. 2017;76:262–74.
113. Krishna GG, Krishna G, Bhalaji N. Analysis of routing protocol for low-power and lossy networks in IoT real time applications. Procedia Comput Sci. 2016;87:270–4.
114. Singh D, Tripathi G, Jara AJ. A survey of internet of things: future vision, architecture, challenge and services. In: Proc. IEEE world forum on internet of things, Seoul, South Korea; 2014. p. 287–92.
115. Jara AJ, Ladid L, Skarmeta A. The internet of everything through Ipv6: an analysis of challenges, solutions and opportunities. J Wirel Mob Netw Ubiquitous Comput Dependable Appl. 2013;4(3):97–118.
116. Madsen H, Burtschy B, Albeanu G, Popentiu-Vladicescu FI. Reliability in the utility computing era: towards reliable Fog computing. In: Proc. 20th international conference on systems, signals, and image processing (IWSSIP); 2013. p. 43–6.
117. Soret B, Pedersen KI, Jorgensen NTK, Fernandez-Lopez V. Interference coordination for dense wireless networks. IEEE Commun Mag. 2015;53(1):102–9.
118. Andrews JG. Seven ways that HetNets are a cellular paradigm shift. IEEE Commun Mag. 2013;51(3):136–44.
119. Jaber M, Imran MA, Tafazolli R, Tukmanov A. 5G Backhaul challenges and emerging research directions: a survey. IEEE Access. 2016;4:1743–66.
120. Choi S, Koh S-J. Use of proxy mobile IPv6 for mobility management in CoAP-based internet of things networks. IEEE Commun Lett. 2016;20(11):2284–7.
121. Maier M, Chowdhury M, Rimal BP, Van DP. The tactile internet: vision, recent progress, and open challenges. IEEE Commun Mag. 2016;54(5):138–45.

122. Fernandes JL, Lopes IC, Rodrigues JJPC, Ullah S. Performance evaluations of RESTful web services and AMQP protocol. In: 5th international conference on ubiquitous and future networks (ICUFN), Da Nang, Vietnam, 2–5 July 2013.

Publisher's Note