Annals of Emerging Technologies in Computing (AETiC)
Vol. 3, No. 3, 2019

Review Article

Survey on Internet of Things (IoT) for Different Industry Environments

Usman Ahmad[1], Junaid Chaudhary[2], Mudassar Ahmad[3,*] and Amjad Ali Naz[3]

[1]Department of Computer Science, Lahore College for Women University, Lahore, Pakistan
Usman.ahmad82@yahoo.com
[2]College of Security and Intelligence, Embry-Riddle Aeronautical University, USA
chaudhrj@erau.edu
[3]National Textile University, Faisalabad, Pakistan
mudassar.utm@gmail.com; nazali4all@hotmail.com
Correspondence: mudassar.utm@gmail.com

Received: 20th May 2019; Accepted: 10th June 2019; Published: 1st July 2019

Abstract: Internet of Things (IoT) provides an opportunity to build powerful applications and computing systems by using wireless communication and radio frequency identification (RFID), mobile, wired and wireless sensor device. In recent years several IoT applications have been developed for industrial use. To comprehend the IoT development, this survey paper provides a precise review of current research on IoT technologies. This study provides IoT applications regarding industries and categorizes the research challenges, issues, and developments. This survey contributes in providing the current state-of-the-art information regarding industrial IoT.

Keywords: ***Internet of Things; IoT; Radio-frequency identification (RFID); WSN; Industry***

1. Introduction

Internet of Things is an emerging technology and expected to provide encouraging solutions to change the procedures and working of recent industrial systems like transportation systems and production system. For example, when IoT is used to develop a smart transportation system, the authority of transportation able to track the vehicle's current position and mobility can forecast the next location and traffic on the road. Initially, the term IoT was introduced to identify interconnected devices by using radio frequency identification (RFID) technology [1]. With the passage of time researchers relate IoT with the number of other technologies such as mobile devices, sensors, GPS devises. A commonly putative description by the researchers for the IoT is an active comprehensive network infrastructure with robust competencies built on interoperable and standard communication protocols. Wherever virtual and physical 'Things' have individual identities, physical and virtual behaviors and attributes having smart interfaces. Furthermore, these are flawlessly integrated into the information and communication network [2]. The implementation of communication technologies, RFID tags and miscellaneous digital/analog sensors are used as the foundation of IoT. It describes how numerous physical objects and sensor devices can stand associated to the Internet.

Usman Ahmad, Junaid Chaudhary, Mudassar Ahmad and Amjad Ali Naz, "Survey on Internet of Things (IoT) for Different Industry Environments", *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 28-43, Vol. 3, No. 3, 1st July 2019, Published by International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2019.03.004, Available: http://aetic.theiaer.org/archive/v3/v3n3/p4.html.

In addition, rules and policies are defined that, in what way these objects and devices are permitted to collaborate and connect with each other to realize mutual objectives [3].

Usage of IoT technologies is growing rapidly in the number of industries [4]. Many projects related to industrial IoT are proposed in areas such as security surveillance, food processing industry, agriculture, environmental monitoring, and many others. Moreover, publications related to IoT are increasing rapidly. In this paper, we have done broad literature review by selecting the related articles on IoT from five renowned academic databases (Science Direct, IEEE Xplore, INSPEC, ACM digital library, Web of Knowledge) to facilitate the readers to comprehend the recent standing and further research activities concerning the IoT usage in an industrial environment. In this survey, our main objective is to identify the breadth and range of recent IoT research in industry and underscoring the issues and prospects for future researchers. We found 396 journal research papers related to IoT published from 2009 to 2017. Figure 1 shows the journal papers stored in Web of Knowledge between 2009 and 2017. Figure 1 also shows that the research trend from 2009 to 2017 is also increasing rapidly.

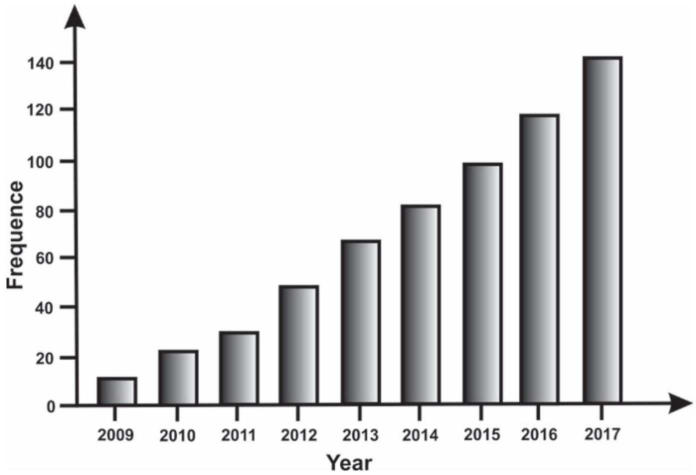

Figure 1. Number of research articles by year.

This survey paper is arranged as follows. Section II describes the contextual background, recent research, and improvements in IoT. Section III discusses the service-oriented architecture of IoT. Section IV shows the analysis of technologies that make IoT possible for working. Section V defines IoT applications which are using in industries. Section VI shows research issues and future developments. Section VII defines the conclusion at the end.

2. Background and Present Research of IoT

IoT is just like an international network based on the number of connected devices with each other and depends on networking, communication and sensory [5]. The initial technology for IoT is the RFID which is used microchips to send data to the sender through the wireless link. Through RFIDs, people can be monitored, tracked and identified. RIFD technology is commonly used in numerous areas like retailing, logistics, and pharmaceutical production. Another fundamental technology for RFID is wireless sensor networks (WSNs), which are used to connect sensors to monitor. The applications used for WSNs are traffic monitoring, environmental monitoring, industrial monitoring and healthcare monitoring [6] [7].

The improvements in wireless sensor networks and RFID significantly contribute to the progressive development of IoT. Moreover, a number of other technologies and devices like near field communication (NFC), ZigBee, cloud computing, smartphones, Wi-Fi, social networking, and barcodes are used to develop a network to support IoT [8] as shown in Fig. 2.

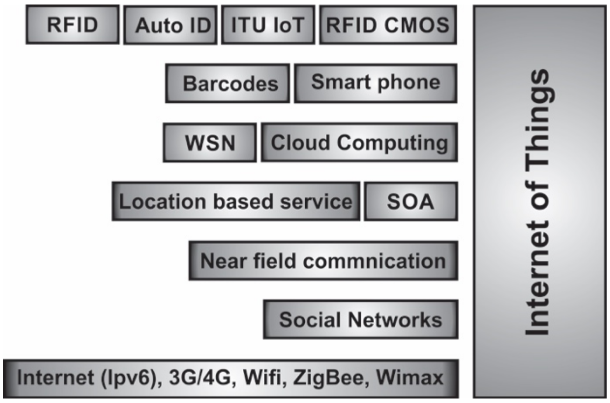

Figure 2. Technologies related to IoT Environment.

However, IoT is gaining attraction in the industry for example in pharmaceutics, logistics, retailing and manufacturing. The number of smart objects and networked things are included in IoT due to rapid development in sensor networks, wireless communication, and smartphones. Due to these developments, IoT related technologies are creating a big impact on enterprise system technologies and information and communication technology (ICT) which are shown in Fig 3.

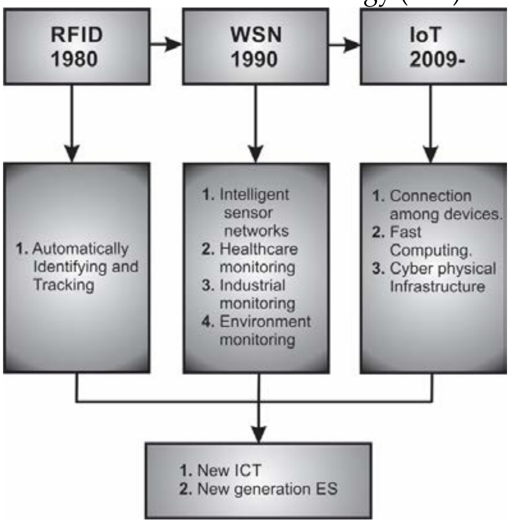

Figure 3. IoT technologies besides the impact on new ICT.

Technical standards for IoT need to develop the step by step communication specifications, processing criterions and for information exchange among the communication things. IoT success depends upon the calibration, which delivers the reliability, real effective operations, interoperability, and compatibility on a worldwide scale [9]. The number of organizations and countries are collaborating with each other and have interest in the growth of industrial IoT standards because the effect of the development of IoT can produce remarkable economic and social benefits in coming era. Recently many companies such as American National Standards Institute, China Electronics Standardization Institute, International Electro-technical Commission, International Telecommunication Union, IEEE, and European Committee for Electro-technical Standardization are working together on the development of many IoT standards [10] [11].

Therefore, several companies are working together for the IoT standardization, a robust harmonization among the various standardization, companies are required to coordinate between national and international standards organizations [12]. With the help of broadly accepted standards and developers, it can possible to use IoT services and applications which can be experienced on a large scale. The number of companies in different countries is invested in IoT technologies. The government of the United Kingdom launched 5 million for the development of IoT. European Research Cluster (IERC) proposed the number of projects related to IoT and launched an international forum for IoT to design and develop a combined technical and strategic image for the development and use of IoT technologies in Europe [13] [14]. China also invests 800 million dollars in the IoT industry by 2016. China has a plan to lead in setting the standards for IoT technologies [15]. Japan has also launched i-japan and u-japan approaches to use IoT technologies in daily life [16].

3. The Service-Based Architecture of IoT

The main objective of IoT is to connect different devices or things over the internet. Service-based architecture is also known as service-oriented architecture (SOA). SOA can also use to support IoT as a main contributing technology in devices or heterogeneous systems. Nowadays SOA is used successfully in the number of research areas including vehicular networks, cloud computing platforms, and wireless sensor networks WSN [17] [18]. Some researchers also proposed the ideas to create multilayer SOA architecture for IoT technologies. According to the International Telecommunication Union, IoT architecture based on five different layers which are sensing, accessing, networking, middleware, and application layers [6] [19]. The number of researchers proposed three major layers for IoT architecture which are perception, network, and service layers. Atzori et al also proposed the three-layer model for IoT architecture which is based on the application, network and the sensing layers [11]. Liu et al also proposed application architecture for IoT which consists of the application, middleware, transport, and physical layers. According to the functionality of layers in IoT, a layered architecture of IoT is shown in Table I. The design consideration for industrial IoT application is illustrated in Table II. The interaction and linkages of four layers with each other are shown in figure 4.

The architectural design of IoT technologies is based on the number of things such as business models, web services, web applications, corresponding process, smart objects, data processing, networking and communication, and security etc. For IoT technologies, the architecture of IoT must ponder the scalability, modularity, extensibility, and interoperability among various devices. The architecture of IoT needs to provide effective and efficient event driven capability due to its decentralized and heterogeneous nature [11] [12] [18].

Table 1. Layered architecture for IoT technology.

Layers	Description
Sensing Layer	To control the physical world and data an existing hardware (RFID, Sensors) are integrated with this layer.
Networking Layer	The functionality of this layer is to provide a basic networking support and data transfer operations over the wireless or wired network.
Service Layer	This layer is responsible of creating and managing services. Services are provided to the users to fulfil their needs.
Interface Layer	This layer provides interactable interfaces and methods services to the users.

Table 2. Design goals for Industrial IoT Applications.

Design goals	Description
Energy	How long can an IoT device operates with limited power supply?
Latency	How much time is a need for message propagation and processing?
Throughput	What is the maximum amount of data that can be transported through the network?
Scalability	How many devices are supported?
Topology	Who must communicate with whom?
Security and Safety	How secure and safe in the application.

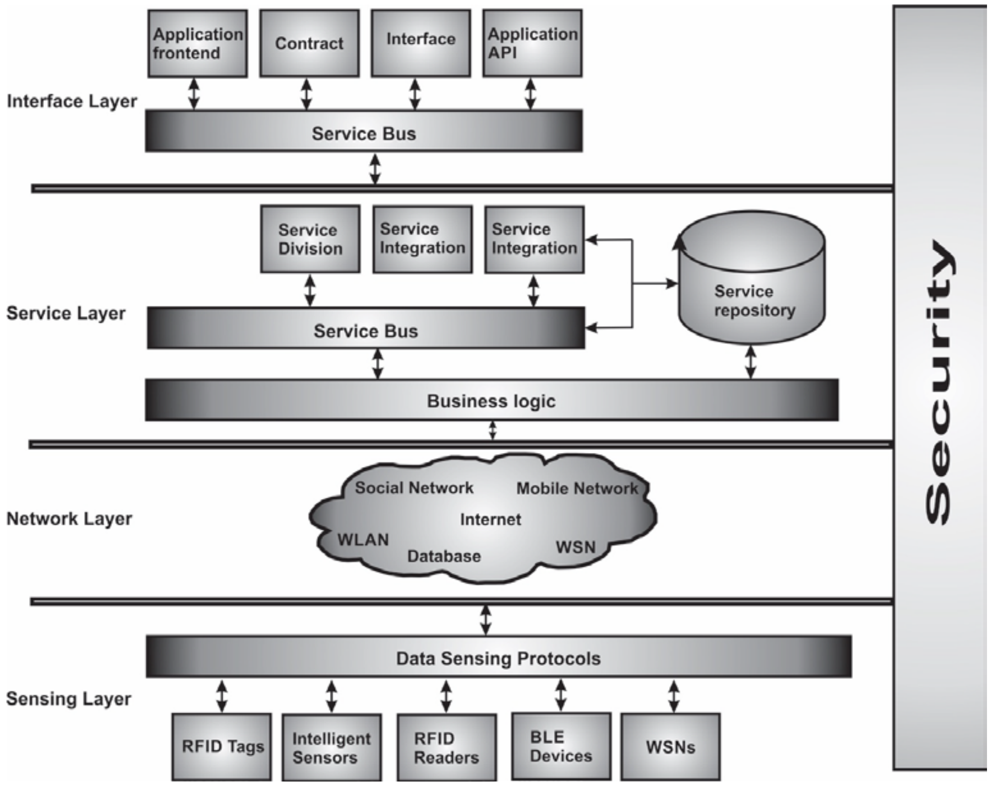

Figure 4. Service-Oriented Architecture for IoT technologies.

3.1. Sensing Layer

IoT can be defined as a worldwide interconnected network, where things or devises are controlled remotely. Interconnected things or devices are become easier, as more and more things are furnished with sensors and RFID technologies [20]. Now Wireless systems along sensors and tags can able to sense and exchange the data between the number of devices, which is controlled by sensing layer. These technologies improve the competency of IoT to identify and sense the things or devices or any other network environment. In the number of industries and companies, the universal unique identifier (UUID) and intelligent service deployment schemes are used to each thing or device or service. A thing or devise equipped with UUID can easily retrieve and identified. However, UUID is the core technology for effective and successful service for a huge IoT Network [20] [21].

3.2. Networking Layer

Networking Layer is responsible to connect all device or things together so that they can able to share the information with each other over the Internet. Moreover, network layer also collects data and information from the present IT infrastructure for example ICT systems, power grids, business systems, healthcare systems, and transportation systems. The IoT services and applications provided by the devices or the things are organized in the diverse heterogeneous network and these all related devices or things provide the serviced Internet [11] [22]. QoS Management may be involved in this process according to the requirements of used applications and users. Moreover, it is very important to discover and map the things or devises automatically in a network especially when the network is dynamic. In IoT, the things must be assigned automatically and scheduled and must be switched to another role automatically when it's needed. These all competencies facilitate the things to work together to complete the given task. For the development of the network layer and its design, developers and researcher must focus and discuss the issues like management of network for heterogenous networks. For an example wired, wireless and mobile networks, QoS requirements, service retrieval, service discovery, energy efficiency requirements in networks, signal and data processing, data and device security and privacy [23].

3.3. Service Layer

This layer depends upon the technology used on the middleware layer which is responsible for functionalities incorporate between applications and services in IoT. This middleware technology also provides a cost-effective and efficient platform for IoT and this platform including software and hardware components which can be reused when needed. The core objective of the service layer is to provide standard service provisions to the middleware, which then are used by different organizations for different applications. An efficient and effective service layer is idealized to identify the application requirements and provide protocols and APIs accordingly to maintain and process the required applications, services, and user requirements. The service layer is also responsible to process all services-based issues, including storage, exchange and management of data, and data communications [11] [12] [23]. Service layer based on the following components.

1. Service APIs: Support the communication among the services needed in IoT [16] [23].
2. Trustworthiness management: This management creates trust and reputation technique which can use and evaluate information which is given by the other services [11] [22].
3. Service composition: service composition creates a relation and communication between connected devices or things. Discovery phase helps to create communication between devices or things to find out the required service, where service composition is responsible to schedule or recreate more appropriate services for the end user request [11] [12].
4. Service discovery: Service discovery is responsible to find objects having needed information or services [11].

3.4. Interface Layer

There is several devices or things are involved in IoT which are made by different companies. These devices do not know the same protocols and standards for communication. Due to this heterogeneous nature, the number of interaction problems occurs during the transfer of information and communication between devices and event processing among the different things. Moreover, it becomes more difficult to connection establishment and operate the things dynamically due to the rapid increase of devices and things in an IoT environment. The core responsibility of the interface layer has also simplified the interconnection and management of things. Interface specific profile can be defined as the subset of services that support interaction with the application used in a network. A user-friendly interface is based on Universal Plug and Play (PnP) implementation, which describes the instruction set (protocol) to facilitate the communication with the services provided by the things [23] [24]. The profile of the interface is used to define the specification among services and application. These services run directly on the service layer to find the new services for an application when it connects to the network. Recently a SOCRADES integration architecture has been developed to efficiently interact among the applications and services [23] [25]. Basically, applications are facilitated by a service layer which provided the universal API. According to the latest research, SOA-IoT reported [26]; interaction among services and applications can be retrieved from the service provisioning process (SPP) efficiently and effectively. To find the required service for application SPP perform "types query" that sends the request for service having WSDL format and after that "candidate search" is used to find the service. With the help of "QoS" and "Application", all service requests are ranked and saved. An "On-demand service provisioning" technique is used to locate service for the application. At the end, process is evaluated through "Process Evaluation" procedure [26] [27].

4. The Key Enabling Technologies

4.1. Tracking and Identification Mechanisms in IoT

The tracking and identification mechanisms used in the IoT environment based on barcodes, intelligent sensors, and RFID. A simple RFID technique based on the combination of RFID tag and RFID reader. Owing its capability to track, trace, identify and physical objects, the use of RFID technology is rapidly increasing in the industry for an example healthcare service monitoring, logistics, and supply chain management [6] [28]. There is a number of other benefits of RFID technology such as providing real-time information about the connected device, improving business efficiency, simplifying the business process, reducing labor cost, and increasing the accuracy of inventory information. Due to these capabilities, RIFD technology is successfully used by the number of manufacturers, retailers, and distributors in industries [7] [8]. The latest development in the RIFD system based on the subsequent features [6] [7] [8] [28]. 1) RFID technology with spread spectrum transmission; and 2) mechanisms of managing RFID applications [7] [8]. Still, there are several chances for the growth of RFID technology-based applications [29]. Moreover, RFID systems can be used with WSNs to trace and track things more effectively and efficiently in real time. Intelligent sensor technologies in wireless computer networks for an example sensor device, sensor tags, independent tags, off-board sensors, electromagnetic sensors, and biosensors further help in the development and implementation of industrial applications and services. More powerful applications can be developed, which are more suitable for the industrial environment through integrating the data attained from smart sensors with RFID data.

4.2. Communication Technologies in IoT

In an IoT environment, there is a number of devices such as much industrial equipment and mobile devices. Different devises have different type of communication, transmission power, data storage capacity, networking, and data processing. For an example, the number of different smartphones has powerful data processing, networking communication, data storage capacity. Heart rate monitor devices have limited computation and communication as compared to smartphones. All these devices can relate to the help of communication technologies and networking. In IoT environment, there are number heterogeneous networks for an example WLAN, wireless mesh networks and WSNs etc. In the process of exchange of information, all these networks help the devices and the things. A gateway provides facility to the number of devices for communication and interaction over the Internet. Gateway also gives power to network knowledge with the help of efficient and effective algorithms. Moreover, a gateway is used to control the number of different complex features during the data communication on the Internet [29].

Different devices have different type of QoS requirements such as security, energy efficiency and the number of other performance metrics. Moreover, several things or devices is depending upon batteries so decreasing the energy consumption for these kinds of devices is the top priority. However, the number of devices which are connected by power supply did not focus on energy saving. Internet protocols for an example IPV6 provide great benefit to IoT environment as it can be possible to give an address to any device directly over the Internet [3] [11] [12]. There are a few core communication protocols used in IoT networks such as IP, IPv6, Machine to Machine, IETF Low power Wireless Personal Area Networks, Multi-hop Wireless Sensor Networks, IEEE 802.15.1, NFC, and ISO 1800 6cEPCclass 1 Gen2 etc.

4.3. Networks Tangled with IoT

There are less cross-layered wireless networks protocols like Ad Hoc Networks (AHNs), Wireless Sensor Network (WSN), and Actuator Networks [22]. Therefore, it is important to revise these protocols before using these in the IoT environment. The reason behind this is because the devices included in the IoT network have different type of computation capabilities, communication, and QoS requirement. On the other hand, wireless sensor networks have the same requirements for network and hardware communication. Moreover, the IoT network is depended upon the Internet for data communication besides, WSNs and AHN doesn't required to be connected to the internet to communicate.

4.4. Service Management in IoT

In service based IoT networks, service can be devolved and designed by three steps [3] [11] [12]: 1) design the services by developing the platforms; 2) selecting the communication capabilities and functionalities of the device, and 3) set up the common set of services. The management of service identification depends upon the object classification and context management. IoT also makes a mirror for an object in IoT networks. IoT is based on context-aware and service-oriented architecture, where any physical or virtual object can communicate with each other in the IoT environment. In service based IoT environment, every component provides its functionality as standard service and by using this standard service the overall efficiency of both network and devices is increased in the IoT network.

5. The Key Industrial Applications of IoT

Applications used in the IoT environment are in its initial stage [11] [12] [18], Though, development of IoT networks is increasing rapidly with the passage of time. Very few IoT applications are developed for industrial environments such as security, transportation, production management, workplace and home support, food supply chain, inventory management, healthcare services, and environmental monitoring. Zori et al. [11] and Miorandi et al [12] proposed the overview of applications of IoT for the diverse type of domains. Here we focus only on the IoT applications used in industrial environment. For the development and design of applications of industrial IoT, needs to consider fancy and different objectives and goals.

For the development of these industrial applications, developers make an adjustment between these objectives and goals to have a steadiness between benefits and cost [48]. Some industrial applications are discussed as follow:

1. Role of IoT in the healthcare industry [30]. There are rapid growth and improvement in healthcare services due to rapid growth in IoT networks. IoT environment has many characteristics such as sensing, global identification, and communication capacities, due to these IoT characteristics all objects such as people, medicine, and equipment monitoring and tracking in healthcare system can be done constantly [31]. Using global connectivity, all of the information related to healthcare systems like diagnosis, management, medication, therapy, recovery, finance, logistics, even daily activity can be actively managed, controlled, and shared efficiently and effectively. For an example, the data related to the patient's organ can be collected and monitored time to time by sensors and then send to the doctor's room. IoT depended healthcare services can be mobile and personalized with the assistance of computable devices for example laptops, mobiles or tablets with the Internet connection (Wifi, 3G etc) [32]. The in-home healthcare (IHH) IoT services development is expedited due to rapid growth and widespread of mobile Internet services [30]. There are two major challenges in IoT networks which are security and privacy.
2. Usage of IoT in Food Supply Chain (FSC) [33]. Now a day the FSC is exceptionally complex and distributed. FSC has big temporal and geographical scale and the number of stakeholders and complex operation processes. This complexity caused the number of problems and issues for public food safety, operational efficiency, and quality management. On the other hand, IoT technologies are there to solve issues such as controllability, visibility, traceability. These IoT technologies can handle the FSC from precise, food manufacture, handling, loading, delivering, and consuming. IoT technology solution for FSC depend upon three parts: a) the field devices for connectivity and for data transmission such as RFID tags/readers, WSN nodes, user interface terminals etc.; b) the backend system such as servers, number of terminals for connections database systems, etc.; and c) an infrastructures for communication such as satellite, cellular, WLAN, Ethernet, power line etc. IoT technologies have reasonable networking capacity and all the elements included in it can be distributed in whole FSC. Moreover, the IoT system can efficiently and effectively use the sensing technologies to monitor and track the whole process of food production. Furthermore, IoT technologies

can use to process raw data and can analyze for further decision making and to improve the business process. Lots of data collected by FSC can be analyzed with the help of Big data analytics and can also be analyzed the challenges related to FSC.

3. Usage of IoT for safe mining production. Mine safety is a gigantic issue for the number of countries because of the working environment in underground mines. With the help of IoT technologies, accidents in underground mines can be prevented and reduced. This technology can sense mine disaster signals for early warning, safety for underground production, and disaster forecasting [34]. In IoT environment the wireless communication such as Wifi or RFID can enable the effective and efficient communication between the surface and unground, mining places can be monitored, tracked and analyzed the concerned safety data to improve the safety measures. Another application is used in IoT system for biological and chemical sensors for initial information about the disaster and about the dangerous working area. These biological sensors are used to get biological information through human organs and body and the chemical sensors are used to detect dangerous dust, destructive gases, and the number of other environmental risky signs which can cause accidents. The safety of wireless devices for information exchange is also an emerging problem in IoT networks so advanced research in need on the safety and security of wireless communication devices especially used in mining production.
4. Usage of IoT in logistics and transportation. According to the research, IoT is playing a very important role in the logistics and transportation industry [11]. Due to development in IoT networks the number of physical objects are using sensors, RFID tags, and barcodes. So that now almost all logistics and transportation companies can track and monitor their moving objects end to end including production, shipping, and distribution [35]. Moreover, IoT technologies offer encouraging resolutions to transfigure automobile services and transportation systems [36]. The usage of powerful networking, sensing, data processing and communication in vehicles is rapidly increased in a few years. Therefore, these IoT technologies can be introduced to enhance the underutilized resources and capabilities among the vehicles on the road and in the parking space. For an example, through IoT technologies, we can track and monitor the movement of a vehicle and can calculate its imminent location. Recently, BMW has developed a smart information system (iDrive) having the different type of sensors and tags for monitoring the conditions of environment like monitoring the location of vehicles, the condition of the road to suggest the drive instructions [37]. Zhang et al. [38] proposed and developed an intelligent monitoring and tracking system for refrigerator truck to measure their inner temperature by using wireless communication, different environment measuring sensors, and RFID tags. In the very near future, we will explore the designing and development process of autopilot techniques for vehicles [39]. The privacy and security are two main issues in the IoT network especially in transportation and logistics because of rapid increment in the development of IoT networks. In IoT networks, more efforts are needed to introduce more effective laws and regulations to secure illegal access or leak of confidential data.
5. Usage of IoT technology in firefighting. IoT technology has a leading role in safety field like firefighting to detect the strong indication of fire and provide a primary warning to save from disasters. In China, a big management system and firefighting information database are developed by using barcodes and RFID tags which are attached to each firefighting product. With the help of wireless communication, sensor networks, RFID tags, video cameras, mobile RFID detectors, firefighting authority and number of other companies can execute automatic identification to realize runtime monitoring, early detection, and efficiently select the resources as needed. The number of researchers is using IoT technology to develop advanced emergency management and firefighting management for the Nation [40]. Recently, Ji and Qi [41] proposed a framework related

to IoT applications for emergency management in China. The design of this IoT application based on the sensing layer, supporting layer, transmission layer, application layer, and platform layer. The platform of this IoT applications is the combination of local and sector-specific emergency systems. Design and establish the standards for the development and implementation of fire IoT is a demanding challenge nowadays.

6. Challenges and Future Trends

According to research, it is acknowledged that IoT applications and technologies are still in development phase [18]. There are several research challenges and issues which are still needed to be addressed for industrial IoT such as security, privacy, and standardization [11] [12]. More effort is required to tackle these issues and challenges for the various industrial environment to safeguard the decent fit of IoT devices and things and better communication. A deep and enough understanding related to industrial features and needs for example, cost, risk, privacy, security is needed for the development and implementation of IoT technology in the industry.

6.1. Technical Challenges

A lot of research has been done in the field of IoT technologies but still, there is a number of issues and technical challenges. Some technical challenges and issues are discussed below:

Design and development of SOA is a gigantic challenge because service depended on devices or things might be face cost limitation and performance. Moreover, scalability and security issues also arise when more devices and physical object are linked to the IoT network. In a situation, when there are many devices then scalability and security are problematic at different echelons. Such as during transmission of data and networking, providing services, and data management and processing [12].

To the extent that the network is concerned, the IoT network is a dense and complicated diverse network, based on the connection through different communication technologies among different types of networks. Presently, there is no generally acknowledged platform which can hide the heterogeneity of communication and network technologies and offers transparent services to IoT applications [12]. Due to bulk transmission of data at the simultaneously can cause the communication issues, recurrent delays, and conflicts. It's a big issue and challenges to develop effective and efficient standards and network technologies to control the huge data transmission within the IoT network. The management of the different type of connected devices in term of collaboration and facilitation among different administrating devices interaction, optimization and identification at the protocol and architectural-levels is a gigantic research problem [9].

As far as a service is concerned, due to the lack of commonly accepted service languages, it's very difficult to make the service integration and development of physical objects resources. The already developed services are incomplete or incompatible due to the heterogeneous network environment and different type of communication techniques [11] [12]. Moreover, object naming services and powerful service discovery methods are needed to design and develop to enhance and improve the IoT technologies [11] [12].

IoT network is usually based on information and communication technologies (ICT) environment and pretentious by all networked devices. A huge work needs to be done for the integration of IoT technology with existing IT systems for unified information infrastructure. Moreover, a huge amount of real-time data flow is produced due to many devices connected with the Internet [42]. This data may not use full until and unless users find some way to analyze and understand it [43]. In an IoT environment, there is a need for robust and dense data analytics skills for mining and analyzing the huge amount of data generated by existing IT systems and IoT applications. Moreover, integration of external resources with IoT devices or things like web services and current software systems requires the development of the number of middleware solutions because of the variation of the application according to the industry environment. Design and development of practical applications in which different types of traditional data are combined with IoT related data can be a gigantic challenge for the different type of industrial environments.

6.2. Standardization

The standardization for IoT is a huge challenge now a day due to rapid growth in IoT network. This standardization plays an important part in the development and extent the IoT technology. IoT standardization has an important role to minimize the access barriers for the different new users and service providers. This minimization improves the compatibility among different systems and applications and enhances the performance of services and users at the advanced level. A vigilant standardization development, coordination, and management efforts are required to assure that applications and devices from different geographical areas across the globe to be able to exchange information [12]. The number of standards is used in IoT networks like identification, communication and security standards which might be facilities to design and extent the IoT technologies. There is a number of issues in IoT standardization including privacy issues, security issues, semantic compatibility, radio access level issues, and compatibility issues [44] [45]. Moreover, industry-specific standards or guidelines to implement IoT technology in the industry are also suggested for easier incorporation for the number of different services.

6.3. Privacy Protection and Information Security

The recognition and extensive growth of different innovative IoT technologies and services will generally depending on information security and confidentiality of data safety, which are two problematic disputes in IoT network because of its organization, complexity, mobility, and flexibility [46]. The number of present technologies is presented for consumer use, nonetheless, these technologies are not suitable for the industry because of safety requirements and strict security. For the secure data transmission and information, current encryption techniques are rooted from WSNs and needed to be reviewed carefully for IoT networks. A strong data encryption technique is needed for IoT networks because the number of daily use devices is connected and can be monitored and traced [11]. Data encryption in IoT networks is more important because the number of attacks on IoT entities is greater as compared to ICT [47] [48] [49]. For an instance, applications of health monitoring collect the data related to patient and sent to the doctor's room over the network. During sending data to doctor's room data can be changed or stolen. An unfailing security encryption technique for IoT environment should be investigated according to following aspects: 1) definition of privacy and security should be designed according to legal, social and culture; 2) reputation and trust technique; 3) host to host encryption in transmission security; 4) user data and communication privacy; and 5) security techniques for application and its services.

6.4. IoT Research Trends

The overall design and development of the IoT network usually track the rapid approach and inflate the current IoT practices and identification like RFID. Intercontinental research collaboration and efforts are desired to discourse the above IoT environment associated issues and challenges [50] [51] [62]. Moreover, to start the research exploration to address the discussed issues and challenges; followings, we have classified a few more research trends:

1. Integration of IoT network with Social Network: According to the researchers, there is a stout concern to improve the data communication between different IoT devices by using social networking. For the integration of social networking, a new paradigm is proposed called Social Internet of This (SIoT) [63]. In IoT, the trend is moving from IoT to Web of Things which will be the new vision for the next research. This technology allows the IoT devices to become active on the Web [52] [53].
2. Designing and development of Green IoT: Lot of devices are connected with each other through wired and wireless network and its sensors, the power dissipation of these sensors (specifically the wireless sensors) is gigantic issue and restraint for enhancement in IoT network [54]. According to current research and networks, there is a need for new energy efficient techniques which can able to reduce the energy consumption during data transmission [55].

3. Context awareness and IoT Middleware: When a large number of sensors are connected to the Internet, it is very difficult and also not possible for users to progression and manipulate the data composed from these sensors. To solve this issue Context-awareness techniques are proposed for an example, IoT middleware is developed to improve the understanding of data generated by sensors and helps to decide what data requirements to be handled, process and manipulate according to the user requirement [64]. Mostly, IoT middleware solutions are not well equipped with context- awareness competencies. The European Union has acknowledged context-awareness as a significant IoT research area and also defined the time frame from 2015 to 2020 for the development of context-aware IoT [65][66].
4. Artificial Intelligence and Smart IoT: Arsénio et al. proposed an idea to design and develop the Internet of Intelligent Things with the help of artificial intelligence into devises and data communication networks [67]. The integration of artificial intelligence into the IoT network can produce more features such as self-protection, self-healing, self-configuration, and self-optimization [57] [58] [68]. Moreover, smart devices will be more efficient, intelligent with more memory, reasoning and processing capabilities in the future [59].
5. Cloud Computing and IoT Networks: Cloud computing provides a better way for devices or things to connect with each other and allows users to access various things on the Internet. Therefore further research trend will be the focus on developing and implementation of new platforms which provide sensing as a service through cloud computing [60] [61].

6. Conclusions

The infrastructure of cyber is already very complex where IoT takes apart with different types of devices having different services like processing, identification, communication, sensing, and networking capabilities. Specifically, the use of actuators and sensors are rapidly increased due to various characteristics like smaller, less expensive, and powerful. According to research Industries have strong concern to develop IoT network and industrial applications to automate the whole system and can also able to control, maintain, manage, and monitor the industry system. IoT network must be used widely in the industry because of the rapid growth in industrial infrastructure and technology. For an example in the food industry, WSN and RFID technology is widely used to automate the whole system for monitoring, tracking and tracing the supply chain and food quality to improve the overall quality of system and food.

This paper focuses and reviews the research based on IoT network and industrial perception. In this paper background and SOA models of IoT networks are discussed and then major technologies are elaborated which might be used in the IoT environment. After that, we discussed a few core industrial applications related to IoT networks and pointed out the research issues and challenges and more developments related to IoT networks. The core contribution of this survey paper is that its emphases on Industrial IoT environment and applications. This paper highlights the issues and challenges to industrial IoT and proposed new research directions for the future industrial IoT researchers.

References

[1] K. Ashton. (2009, Jun.). Internet of things. RFID J. Available: http://www.rfidjournal.com/articles/view?4986

[2] R. van Kranenburg, The Internet of Things: A Critique of Ambient Technol- ogy and the All-Seeing Network of RFID. Amsterdam, The Netherlands: Institute of Network Cultures, 2007.

[3] R. van Kranenburg, E. Anzelmo, A. Bassi, D. Caprio, S. Dodson, and M. Ratto, "The internet of things," in Proc. 1st Berlin Symp. Internet Soc., Berlin, Germany, 2011, pp. 25–27.

[4] Y. Li, M. Hou, H. Liu, and Y. Liu, “Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of Internet of Things,” Inf. Technol. Manage., vol. 13, no. 4, pp. 205–216, 2012.

[5] L. Tan and N. Wang, “Future internet: The internet of things,” in Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE), Chengdu, China, Aug. 20–22, 2010, pp. V5-376–V5-380.

[6] S. Li, L. Xu, and X. Wang, “Compressed sensing signal and data acquisition in wireless sensor networks and internet of things,” IEEE Trans. Ind. Informat., vol. 9, no. 4, pp. 2177–2186, Nov. 2013.

[7] W. He and L. Xu, “Integration of distributed enterprise applications: A survey,” IEEE Trans. Ind. Informat., vol. 10, no. 1, pp. 35–42, Feb. 2014.

[8] D. Uckelmann, M. Harrison, and F. Michahelles, “An architectural ap- proach towards the future internet of things,” in Architecting the Internet of Things. D. Uckelmann, M. Harrison, and F. Michahelles, Eds., New York, NY, USA: Springer, 2011, pp 1–24.

[9] D. Bandyopadhyay and J. Sen, “Internet of things: Applications and challenges in technology and standardization,” Wireless Pers. Commun., vol. 58, no. 1, pp. 49–69, 2011.

[10] ITU NGN-GSI Rapporteur Group, Requirements for Support of USN Applications and Services in NGN Environment, Geneva, Switzerland: International Telecommunication Union (ITU), 2010.

[11] Wan, Jiafu, et al. "Software-defined industrial internet of things in the context of industry 4.0." IEEE Sensors Journal 16.20 (2016): 7373-7380.

[12] D. Miorandi, S. Sicari, F.DePellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” Ad Hoc Netw., vol. 10, no. 7, pp. 1497–1516, 2012.

[13] O. Vermesan, P. Friess, and P. Guillemin. (2009). Internet of things strategic research roadmap. The Cluster of European Research Projects. Available: http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf.

[14] H. Sundmaeker, P. Guillemin, and P. Friess, Vision and Challenges for Realizing the Internet of Things. Brussels, Belgium: European Commission, 2010.

[15] K. Voigt. (2012). China Looks to Lead the Internet of Things. Available: http://www.cnn.com/2012/11/28/business/china-internet-of-things/.

[16] H. Zhang and L. Zhu, “Internet of things: Key technology, architecture and challenging problems,” in Proc. 2011 IEEE Int. Conf. Comput. Sci. Autom. Eng. (CSAE), Shanghai, China, Jun. 10–12, pp. 507–512.

[17] Borgohain, Tuhin, Uday Kumar, and Sugata Sanyal. "Survey of security and privacy issues of Internet of Things." arXiv preprint arXiv:1501.02211 (2015).

[18] L. Xu, “Enterprise Systems: State-of-the-art and future trends,” IEEETrans. Ind. Informat., vol. 7, no. 4, pp. 630–640, Nov. 2011.

[19] Karagiannis, Vasileios, et al. "A survey on application layer protocols for the internet of things." Transaction on IoT and Cloud Computing 3.1 (2015): 11-17.

[20] Y. Wu, Q. Z. Sheng, and S. Zeadally, “RFID: Opportunities and chal- lenges,” in Next-Generation Wireless Technologies, N. Chilamkurti, Ed. New York, NY, USA: Springer, 2013, ch. 7, pp. 105–129.

[21] E. Ilie-Zudor, Z. Kemeny, F. van Blommestein, L. Monostori, and A. van der Meulen, “A survey of applications and requirements of unique identifi- cation systems and RFID techniques,” Comput. Ind., vol. 62, no. 3, pp. 227–252, 2011.

[22] C. Han, J. M. Jornet, E. Fadel, and I. F. Akyildiz, “Across-layer communi- cation module for the internet of things,” Comput. Netw., vol. 57, no. 3, pp. 622–633, 2013.

[23] Faheem, Muhammad, and V. C. Gungor. "MQRP: Mobile sinks-based QoS-aware data gathering protocol for wireless sensor networks-based smart grid applications in the context of industry 4.0-based on internet of things." Future Generation Computer Systems (2017).

[24] K. Gama, L. Touseau, and D. Donsez, "Combining heterogeneous service technologies for building an internet of things middleware," Comput. Commun., vol. 35, no. 4, pp. 405–417, 2012.

[25] D. Romero, G. Hermosillo, A. Taherkordi, R. Nzekwa, R. Rouvoy, and F. Eliassen, "RESTful integration of heterogeneous devices in pervasive environments," in Distributed Applications and Interoperable Systems. Berlin, Germany: Springer-Verlag, 2010, ch. 01, pp. 1–4.

[26] Trappey, Amy JC, et al. "A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0." Advanced Engineering Informatics (2016).

[27] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (SIoT)-when social networks meet the internet of things: Concept, archi- tecture and network characterization," Comput. Netw., vol. 56, no. 16, pp. 3594–3608, 2012.

[28] Ben-Daya, Mohamed, Elkafi Hassini, and Zied Bahroun. "Internet of things and supply chain management: a literature review." International Journal of Production Research (2017): pp 1-24.

[29] Dong, Xinping, and Caihong Ye. "Analysis on growth mechanism of the internet of things industrial cluster." RISTI (Revista Iberica de Sistemas e Tecnologias de Informacao) E10 (2016): 453-463.

[30] Z. Pang,Q. Chen, J. Tian, L. Zheng, and E.Dubrova, "Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things," in Proc. 2013, 15th Int. Conf. Adv. Commun. Technol. (ICACT), Pyeongchang, Korea, pp. 529–534.

[31] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," Comput. Netw., vol. 54, no. 15, pp. 2688–2710, 2010.

[32] I. Plaza, L. Martín, S. Martin, and C. Medrano, "Mobile applications in an aging society: Status and trends," J. Syst. Softw., vol. 84, no. 11, pp. 1977–1988, 2011.

[33] Perera, Charith, et al. "A survey on internet of things from industrial market perspective." IEEE Access 2 (2014): 1660-1679.

[34] Pang, Zhibo, et al. "Value-centric design of the internet-of-things solution for food supply chain: Value creation, sensor portfolio and information fusion." Information Systems Frontiers 17.2 (2015): 289-319.

[35] B. Karakostas, "A DNS architecture for the internet of things: A case study in transport logistics," Procedia Comput. Sci., vol. 19, pp. 594–601, 2013.

[36] H. Zhou, B. Liu, and D. Wang, "Design and research of urban intelligent transportation system based on the internet of things," Commun. Comput. Inf. Sci., vol. 312, pp. 572–580, 2012.

[37] E. Qin, Y. Long, C. Zhang, and L. Huang, "Cloud computing and the internet of things: Technology innovation in automobile service," LNCS 8017, New York, NY, USA, 2013, pp. 173–180.

[38] Y. Zhang, B. Chen, and X. Lu, "Intelligent monitoring system on refrigera- tor trucks based on the internet of things," Wireless Commun. Appl., vol. 72, pp. 201–206, 2012.

[39] C. G. Keller, T. Dang, H. Fritz, A. Joos, C. Rabe, and D.M.Gavrila, "Active pedestrian safety by automatic braking and evasive steering," IEEE Trans. Intell. Transp. Syst., vol. 12, no. 4, pp. 1292–1304, Dec. 2011.

[40] Y. C. Zhang and J. Yu, "A study on the fire IOT development strategy," Procedia Eng., vol. 52, pp. 314–319, 2013.

[41] Z. Ji and A. Qi, "The application of internet of things (IOT) in emergency management system in China," in Proc. 2010 IEEE Int. Conf. Technol. Homeland Security (HST), pp. 139–142.

[42] S. Wang, Z. Zhang, Z. Ye, X. Wang, X. Lin, and S. Chen, “Application of environmental internet of things on water quality management of urban scenic river,” Int. J. Sustain.Develop.WorldEcol., vol. 20, no.3, pp. 216–222, 2013.

[43] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, “Context aware computing for the internet of things: A survey,” IEEE Commun. Surveys Tuts., to be published.

[44] F. Wang, B. Ge, L. Zhang, Y. Chen, Y. Xin, and X. Li, “A system frameworkof securitymanagement in enterprise systems,” Syst. Res. Behav. Sci., vol. 30, no. 3, pp. 287–299, 2013.

[45] Y. Xing, L. Li, Z. Bi, M. Wilamowska-Korsak, and L. Zhang, “Operations research (OR) in service industries: A comprehensive review,” Syst. Res. Behav. Sci., vol. 30, no. 3, pp. 300–353, 2013.

[46] J. Wan and J. Jones, “Managing IT service management implementation complexity from the perspective of the Warfield version of systems science,” Enterp. Inf. Syst., vol. 7, no. 4, pp. 490–522, 2013.

[47] Granjal, Jorge, Edmundo Monteiro, and Jorge Sá Silva. "Security for the internet of things: a survey of existing protocols and open research issues." IEEE Communications Surveys & Tutorials 17.3 (2015): 1294-1312.

[48] Pang, Zhibo, et al. "Design of a terminal solution for integration of in-home health care devices and services towards the Internet-of-Things." Enterprise Information Systems 9.1 (2015): 86-116.

[49] Islam, SM Riazul, et al. "The internet of things for health mprehensive survey." IEEE Access 3 (2015): 678-708.

[50] J. Clarke, R. Castro, A. Sharma, J. Lopez, and N. Suri, “Trust & security RTD in the internet of things: Opportunities for international cooperation,” in Proc. 1st Int. Conf. Security of Internet of Things, Kollam, India, 2012, pp. 172–178.

[51] Harwood, T., Harwood, T., Garry, T., & Garry, T. (2017). Internet of Things: understanding trust in techno-service systems. Journal of Service Management, 28(3), 442-475.

[52] Madakam, Somayya, R. Ramaswamy, and Siddharth Tripathi. "Internet of Things (IoT): A literature review." Journal of Computer and Communications 3.05 (2015): 164.

[53] Tran, N. K., Sheng, Q. Z., Babar, M. A., & Yao, L. (2017). Searching the Web of Things: State of the Art, Challenges, and Solutions. ACM Computing Surveys (CSUR), 50(4), 55.

[54] Lee, In, and Kyoochun Lee. "The Internet of Things (IoT): Applications, investments, and challenges for enterprises." Business Horizons 58.4 (2015): 431-440.

[55] Wang, K., Wang, Y., Sun, Y., Guo, S., & Wu, J. (2016). Green industrial Internet of Things architecture: An energy-efficient perspective. IEEE Communications Magazine, 54(12), 48-54.

[56] Bello, O., & Zeadally, S. (2016). Intelligent device-to-device communication in the internet of things. IEEE Systems Journal, 10(3), pp 1172-1182..

[57] Tao, Fei, Jiangfeng Cheng, and Qinglin Qi. "IIHub: an Industrial Internet-of-Things Hub Towards Smart Manufacturing Based on Cyber-Physical System." IEEE Transactions on Industrial Informatics (2017).

[58] Zuo, Y., Tao, F., & Nee, A. Y. C. (2017). An Internet of things and cloud-based approach for energy consumption evaluation and analysis for a product. International Journal of Computer Integrated Manufacturing, 1-12.

[59] Kshetri, Nir. "The evolution of the internet of things industry and market in China: An interplay of institutions, demands and supply." Telecommunications Policy 41.1 (2017): 49-67.

[60] Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. (2017). Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. IEEE wireless communications, 24(3), 10-16.

[61] Martellini, Maurizio, et al. "Assessing Cyberattacks Against Wireless Networks of the Next Global Internet of Things Revolution: Industry 4.0." Information Security of Highly Critical Wireless Networks. Springer International Publishing, 2017 pp 63-69.

[62] Junaid Chaudhry, Uvais Qidwai and Mahdi H. Miraz, "Securing Big Data from Eavesdropping Attacks in SCADA/ICS Network Data Streams Through Impulsive Statistical Fingerprinting", Proceedings of the 2nd International Conference on Emerging Technologies in Computing 2019 (iCETiC'19), London Metropolitan University, UK, Part of the Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), DOI: 10.1007/978-3-030-23943-5_6.

[63] Mahdi H. Miraz, Maaruf Ali, Peter S. Excell and Rich Picking, "Internet of Nano-Things, Things and Everything: Future Growth Trends", in Future Internet, ISSN: 1999-5903, Volume 10, Issue 8, Paper No. 68, Published by MDPI. DOI: 10.3390/fi10080068, 27 July 2018. Available: http://www.mdpi.com/1999-5903/10/8/68.

[64] Mahdi H. Miraz, Maaruf Ali, Peter Excell and Rich Picking, "A Review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)", in the proceedings of the fifth international IEEE conference on Internet Technologies and Applications (ITA 15), Glyndŵr University in Wrexham, UK, DOI: 10.1109/ITechA.2015.7317398, Print ISBN: 978-1-4799-8036-9, pp 219-224, 8-11 September 2015, Published by IEEE, Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7317398.

[65] Mahdi H. Miraz, "Blockchain of Things (BCoT): The Fusion of Blockchain and IoT Technologies", in "Advanced Applications of Blockchain Technology", published by Springer Nature, DOI: 10.1007/978-981-13-8775-3_7.

[66] Zainab Alansari, Nor Badrul Anuar, Amirrudin Kamsin, Safeeullah Soomro, Mohammad Riyaz Belgaum, Mahdi H. Miraz and Jawdat Alshaer, "Challenges of Internet of Things and Big Data Integration", in the proceedings of the International Conference on Emerging Technologies in Computing 2018 (iCETiC '18), 23-24 August 2018, London Metropolitan University, London, UK, Part of the Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), vol. 200, Online ISBN: 978-3-319-95450-9, Print ISBN: 978-3-319-95449-3, Series Print ISSN: 1867-8211, Series Online ISSN: 1867-822X, DOI: 10.1007/978-3-319-95450-9_4, pp. 47-55, Published by Springer-Verlag, Available: https://link.springer.com/chapter/10.1007/978-3-319-95450-9_4.

[67] Mahdi H. Miraz and Maaruf Ali, "Blockchain Enabled Enhanced IoT Ecosystem Security", in the proceedings of the International Conference on Emerging Technologies in Computing 2018 (iCETiC '18), 23-24 August 2018, London Metropolitan University, London, UK, Part of the Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), vol. 200, Online ISBN: 978-3-319-95450-9, Print ISBN: 978-3-319-95449-3, Series Print ISSN: 1867-8211, Series Online ISSN: 1867-822X, DOI: 10.1007/978-3-319-95450-9_3, pp. 38-46, Published by Springer-Verlag, available: https://link.springer.com/chapter/10.1007/978-3-319-95450-9_3.

[68] Syamsul H. Mahmud, Laromi Assan and Rashidul Islam, "Potentials of Internet of Things (IoT) in Malaysian Construction Industry", Annals of Emerging Technologies in Computing (AETiC), Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 44-52, Vol. 2, No. 1, 1st October 2018, Published by International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2018.04.004, Available: http://aetic.theiaer.org/archive/v2/v2n4/p4.pdf.