IRAQI JOURNAL FOR COMPUTERS AND INFORMATICS
IJCI
Vol. [46], Issue [1], Year (2020)

A REVIEW ON INTERNET OF THINGS ARCHITECTURE FOR BIG DATA PROCESSING

Wid Akeel Awadh [1]
[1] *Computer Information Systems Department*
University of Basrah
Basrah, IRAQ
umzainali@gmail.com

Ali Salah Hashim[2]
[2]*Computer Science Department*
University of Basrah,
Basrah, IRAQ
alishashim2009@gmail.com

Alaa Khalaf Hamoud[3]
[3]*Computer Information Systems Department*
University of Basrah.
Basrah, IRAQ
alaa.hamoud@uobasrah.edu.iq

***Abstract* - The importance of big data implementations is increased due to large amount of gathered data via the online gates. The businesses and organizations would benefit from the big data analysis i.e. analyze the political, market, and social interests of the people. The Internet of Things (IoT) presents many facilities that support the big data transfer between various Internet objects. The integration between the big data and IoT offer a lot of implementations in the daily life like GPS, Satellites, and airplanes tracking. There are many challenges face the integration between big data transfer and IoT technology. The main challenges are the transfer architecture, transfer protocols, and the transfer security. The main aim of this paper is to review the useful architecture of IoT for the purpose of big data processing with the consideration of the various requirements such as the transfer protocol. This paper also reviews other important issues such as the security requirements and the multiple IoT applications. In addition, the future directions of the IoT-Big data are explained in this paper.**

Index Terms – IoT, Big Data, Protocols, Security, Multiple applications.

I. INTRODUCTION

Recently, the IoT become one of the most interest domains in the research of technology industry. IoT can be described as the internet communication between things in real life, whereby the data would be gathered among any defined "things" in the internet network [1]. The IoT facilities allow the identification of the real things as digital objects. Thus, these objects can interact with each other through gathering the data via the internet network. Many reports that produced from known companies (such as Cisco and Ericsson) mentioned that it is expected to record about 50 billion connected and interacted things by the end of 2020 [2]. Hence, the IoT network could produces large implementations that act with the human life. Examples of these implementations the smart health services, monitoring the road traffic, track the supply chains, and etc. Simply put, IoT able to represent the life things by digital sensors and the connections between these sensors able to create several systems to serve the human needs [3]. One of the main advantages of the IoT is responsible networks costs due to the ability to reuse the current networks facilities in order to obtain the communication between the "things". The extending in the IoT is the users or "things" representation by digital sensors and the required connection methods between these things. Table I summarizes the main standard definitions of the IoT by known organizations.

TABLE I
MAIN STANDARD DEFINITIONS OF IOT

Standard	IoT Definition
(CCSA)	Gather information between life objects using network, collect the gathered information, processes and analyze the information, and produce a real act or service [4].
(ITU-T)	Global network facilities applied to offer communication between virtual or physical objects in the life. The network technology is able to processes the manage the communication between the objects based on the gather information via the objects network [5].
EU FP7	Acquire and process data from defined objects using global communication between these objects. [6].
CASAGRAS	A global communication between defined objects in the life depend on useful communication protocols [7].

Although, the IoT technology offers advantages to innovate large amount of implications, the IoT facilities could face challenges in cover the data transfer of some applications. For example, the bandwidth of the IoT devices and communication may face challenge in transfer/process large amount of data among the "things" [8]. This challenge is an issue in the application of big data such as aircraft industry, which gather data of huge capacity. Thus, the IoT facilities need to be equipped by useful bandwidth transfer facilities in order to present adapted solutions for the big data applications [9]. Even the applications that deal with objects of small data may convert to big data applications when it offers communication between large numbers of objects i.e. Millions of devices. The big data processing brings many issues such as the transfer management protocol and the security of the transfer data. For this reason, the IoT architecture should be designed to manage effectively using suitable management protocols under the condition of data security.

Based on the above challenge, this paper aims to review the architecture of the IoT for useful applications of big data, where by the integration between the IoT and big data will more applicable. This paper consists of seven main sections; the next section clarifies the importance and challenges of the integration between the IoT and Big data. Section 3 explains the models that can be adopted to manage the IoT communications. Section 4 presents the main layers of IoT architecture. Section 5 discusses the management protocols of the IoT. Section 6 clarifies the security requirements of IoT. The IoT implications for big data are clarified in section 7. Lastly, section 8 presents the conclusion and the future works.

II. OVERVIEW OF BIG DATA SUPPORTING IOT

The concept of big data can be determined by three main factors [10]; (1) the large volume of data transfer, (2) the variety of data i.e. structured and unstructured, and (3) the speed of data transfer. In the other words, the application is considered as big data if it allows the transfer of large volume of data. The transfer data may take any form and format i.e. database, audio, videos, images, or books. The transfer of big data should be arrived to destination at real time. Hence, the network facilities must address these three determinants of the big data applications. The IoT network is efficient to reduce the physical cost of the applications due to reusing of existing network equipments [10][11]. However, the IoT network could faces challenges in handle the big data transfer. The IoT facilities need to have sufficient bandwidth, allow the data transfer of various structures, and able to transfer the big data at real time. Without these requirements, the Big data application may fail due to drawbacks in the services. In this context, the main success key of the IoT is to assure effective equipments for big data platform in order to gather, acquire, and process large amount of data at real time [10].

The network data management is usually conducted based on ELT approach (extract, transform, and load data) [12]. ETL works on acquire/extract data from various network sources, transfer the data to standard format to simplify the data analysis, and load the data to database for further processing to produce services. The ELT is conducted based on two related stages; (1) acquire and store the data, and (2) manage and process the data [10]. These two stages are useful to assure the system flexibility. New objects or devices can be added in relation with storing stage and the services could be added/updated in relation with management stage. Furthermore, The ELT approach works on speed up the data processing through standardized the data structure to simplify the data processing, whereby the IoT could integrated effectively with the big data applications. The nature of big data is requires parallel processing methods such as MPI, GPU, and MapReduce [13]. These methods are working effectively on the managed or centralized big data like the managed data in the second stage of ELT approach. In conclusion the ELT could useful approach to manage the big data transfer using distributed IoT infrastructures.

Put ELT approach together with IoT and big data applications, the large number of IoT objects work on gather the data with central management database. In the first stage of ELT, the big data is acquired from the IoT objects and stored in the database based on standard format. In the second ELT stage, the IoT facilities works on processes and analyze the stored data in order to produce efficient services for the destination devices [14]. The conducted services should be delivered for the destinations at real time and in right context. One of the most known management system of big data is the Hadoop/MapReuce [15, 16]. The Hadoop tool works on acquire and store the data from multiple network sources. On the other hand, the MapReduce tool works on process the collected data to optimize the solutions based on the data patterns. However, the data security is one of main drawbacks of Hadoop tool due to lack in encrypt the collected data from the network sources [16]. Thus, The IoT network need to assure the data security through secures the communication paths between the various connected objects. The next section presents some IoT models that can be adopted depend on different communication modes to serve the applications.

III. COMMUNICATION MODELS OF IOT

As mentioned in Section 1, the IoT is a technology that applied to communicates between virtual or physical objects in order to provide services based on the gathered data among these objects. The IoT could integrate with big data applications under three main conditions that are the transfer of large amount data, transfer of various data structures, and the data transfer at real time. Thus, it is important to adopt effective communication mode to serve the big data applications by IoT technology. This section clarifies the main communication modes of IoT. The communication model can be adopted based on the nature of big data application in order to assure the connection at anytime, from anyplace, and transfer the data at real time. The communication mode can be described as the way that the IoT devices are connected and gather the data among each other. Therefore, The following are the most known communication models of the IoT, which determine the communication mode between the devices [17, 18].

- The Device-to-Device (D2D) Communication Model: in this model the devices are connected directly with each other without critical transfer protocols. The D2D model is required few network infrastructures to accomplish the data transfer among the devices. In this model, the communication mode is performed using the IP address of the devices. Examples of D2D model are the "Bluetooth, ZigBee, or Z-Wave". Figure 1 shows the main structure of D2D communication model.

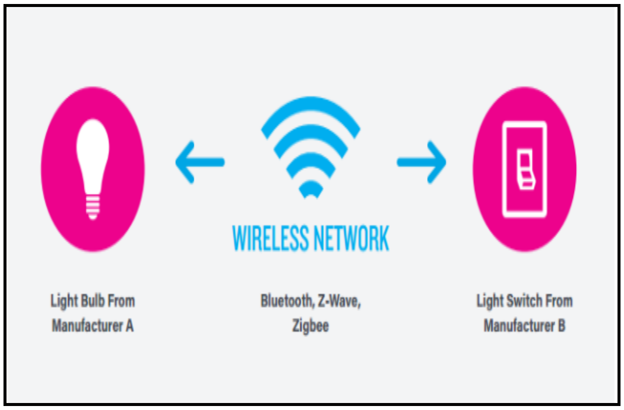

Fig. 1. D2D Communication Model.

- The Device-to-Cloud (D2C) Communication Model: this model is applied to direct connection between the IoT objects and specific cloud services to manage the gathered data via the IoT network. For example, some cloud services are applied to manage the transfer traffic of the data. D2C model performs the communication based on devices IPs that defined in advance by the network. The most known communication modes of D2C model are the Ethernet or Wi-Fi connections. Figure 2 shows the main structure of D2C communication model.

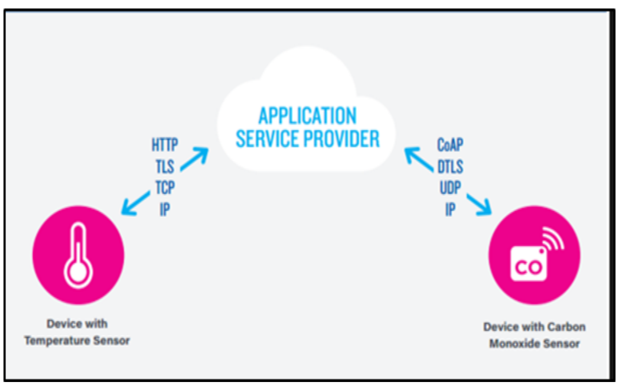

Fig. 2. D2C Communication Model.

- The Device-to-Gateway (D2G) Model: In D2G model, the devices of the IoT are connected to the cloud services through mediating layer that called "Application Layer Gateway" (ALG). The ALG works on reach the cloud services based on trusted transfer protocols. In the other meaning, The ALG is a tool that used to manage the data transfer between the IoT devices and the cloud services and the main goal of this tool is to improve the data transfer security in addition to speed up the data transfer processes. Figure 3 shows the main structure of D2G communication model.

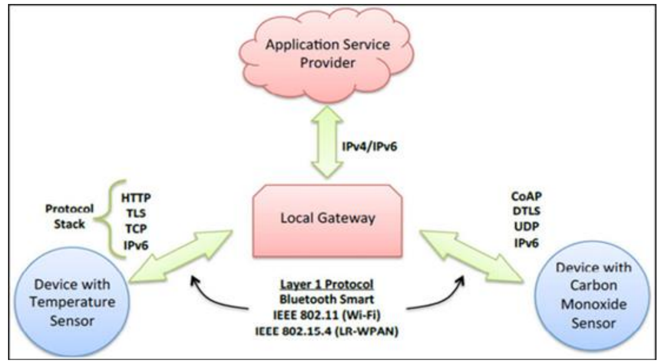

Fig. 3. D2G communication Model.

- The Back-end Data-sharing (BeDs) model: the BeDs model works on collect the data directly from specific IoT device and process the collected data by the cloud service. BeDs is considred as extended from D2C communication model, but the main difference is that the D2C offer data collecting from all IoT devices and the BeDs collect the data from single or specific device. Hence, the BeDs is more fixable than D2C model in analyze the collected data form customized devices. BeDs uses communication modes such as "cloud applications programmer interfaces" (APIs) In order to perform the data transfer between the IoT and cloud. Figure 4 shows the main structure of BeDs communication model.

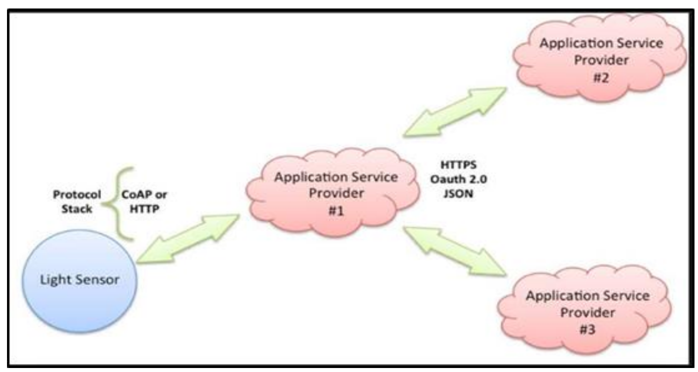

Fig. 4. Back-End Data-Sharing Model.

IV. ARCHITECTURE OF IOT LAYERS

The IoT is defined as a wave of the global network that applied to connect many types of objects in anytime and from anyplace using effective communication mode [19]. The IoT architecture consists of many structured layers to perform the data transfer between the IoT and the cloud [20]. Some works explains three main IoT layers [20]. Other works define four layers of IoT [21], and in some works the IoT is structured as five main layers [22]. In this section the IoT architecture is explains as six main layers [23]. Figure 5 summarizes the six layers of IoT architecture and the next sub-sections points explained each layer responsibility.

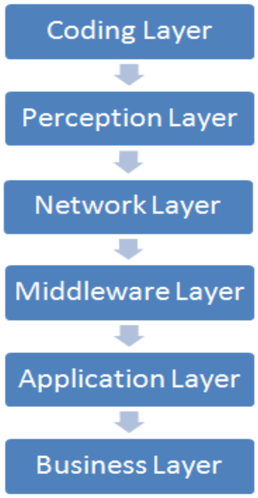

Fig. 5. Main layers of IoT architecture.

A. *Coding Layer*

This layer is the base layer that provides definition for IoT. All information collected from the coding layer is used to define the connection algorithm in order to improve the data transfer rate. The coding layer is useful for determining the requirements of transfer data rate for each device, due to the heterogeneity of the Internet of Things [23, 24].

B. *Perception Layer*

This layer is essentially the physical layer, which includes the electronic tags that sensing the IoT objects, RFID sensors to gather the data between the tags and the workstation, and the super nodes to strength the coverage area of RFID sensors. As a result, the perception layer works on gather the data between the IoT object and the network layer [25].

C. *Network Layer*

This layer is the advanced layer in the IoT architecture [19]. This layer responsible about receives the data from the IoT objects in perception layer. The received data transfers to application layer via communication mode such as Bluetooth, WiFi, and Ethernet; the data transfers is conducted based on protocols such as DDS, IPv4, and IPv6 [26].

D. *Middleware Layer*

Middleware hides the complexities of the lower layers, like network, in order to ease the integration of new and legacy systems. It allows the "things" and the application layer to connect without having to worry about the different operating systems, networks or resources server layers [22].

E. *Application Layer*

This layer understands all kinds of industry in IOT applications. The application layer is necessary to develop large level of Internet of Things. The data received from the network layer, managed in database, processed in meaningful pattern, and create services based on the data processing [22].

F. *Business Layer*

This layer is important to present the conducted services in real time and in right context. The business layer works on manages the processed data as services and delivered these services form the destinations backwards through the network layer [2].

V. TESTING OF IOT COMMUNICATION PROTOCOLS

As explained earlier in this paper, the communication models of IoT are conducted based on several transfer protocols. These protocols need to be tested in order to assure the effectiveness of transfer the big data (transfer large data volume, different structure of data, and data arriving at real time). This section presents the most known testing tools of IoT communication protocols. The first known testing tool is called "Net2Plan", which is open source code that used to test the suitability of the network protocol to serve data transfer [27]. The main advantage of "Net2Plan" tool is the ability to test the various types and architectures of the networks. This tool allows the programmers to customize their testing algorithms to tack the network environment while the data transfer processes is conducted. This tool reports the network status such as the transfer delay, fail, and routing. The reports also generate other results such as network traffic, resources allocation, and manage the transfer paths [27].

Another testing tool for IoT communication protocols is called "EuWIn". This tool works on test the IoT applications based on standard such as "Software Defined Wireless Networking (SDWN), ZigBee and IPv6". The SDWN is applied to enhance the transfer rate for the static and semi-static device allocation, while the ZigBee is suitable for dynamic devices allocation like mobile [28]. Furthermore, the "SensorHUB" is testing toll for IoT communication protocols. This tool can be applied to test the network management of data transfer in addition to analyze the data transfer in different network layers and node. Thus, this tool offer deep testing of the IoT for advanced applications such as big data [29]. The above testing tools could be used to assure the IoT effectiveness in transfer the Big Data based on the requirements of big data applications. However, the IoT-Big data application required other requirements such as the data security. The Security of IoT is explains in the next section.

VI. SECURITY OF IOT

The network security is one of the most important requirements of the data transfer. Thus, the IoT security is very important issue, especially in hard challenge applications such as the big data. The unsafe IoT application may lead to the fail of the applications [30]. For example, in 2016 the attackers were success in breakdown the accessing of some sites through create large number of virtual IoT device to hold the DNS providers for the targeted sites. Like these attacks may cost the businesses due to break the services and lost the customers. According to [31], the security is important for all IoT layers (low, middle, and high layers). The attacks may happen on perception, application, network, middleware, or business layer. Thus, it is important to analyze the different attacks scenarios that could happen on IoT layers in order to improve the security solutions for IoT applications.

The IoT security importance is increased when the big data applications are applied [32]. In IoT-Big data applications, the security methods and approaches should be more efficient due to large amount of transfer data. The transfer of big data required data transfer using more facilities, more network paths, and speeder transfer rate. Thus, the attacks scenarios can be increased due to larger choices of attack the data. [32] Discussed the SDN architecture supporting the Openflow framework in order to improve the security of IoT network for Big data applications. The next section clarifies important applications for IoT-Big data. Table II lists some of security issues related to IoT and how the researchers handled them throughout proposing techniques, explaining requirements, and listing the concerns.

TABLE II
IOT SECURITY ISSUES

Reference	Year	Domain	Details
[33]	2019	Securing System	A proposed IoT secured system which prevents the attackers from permeation through IoT devices. The system secured transmitted data among IoT devices. A details about how the representational state transfer API securing the connection between devices and cloud application.
[34]	2015	Security Requirement	The security requirements of the IoT components that make the system of smart home are described.
[35]	2016	Data Privacy	A research project ARMOUR is proposed where a methodology of experimenting different solutions in a large-scale environment. Besides, many experimental software programs are proposed to explore the security scenarios in IoT environment.
[36]	2019	End-To-End	A novel security model is proposed for IoT that can be utilized by organizations to implement end-to-end connection. The proposed TIotSAM is expanding new features of data gathering and security issues based on Software Assurance Maturity Model.
[37]	2017	Authentication and Authorization	A new component OAuth 2.0-based oneM2M to provide two essential security issues (authorization and authentication) and secure the interconnecting among platforms of IoT.
[38]	2014	Multi-Hop routing	A new proposed multi-hop protocol is proposed to secure IoT interconnected devices. The protocol provide authentication mechanism based parameters of multi-layer for IoT devices. The experiments show that this protocol can be deployed in IoT environment.
[39]	2015	Fragment	The fragment challenge is handled using a framework of agents that deployed in the gateway to communicate with different IoT devices using different protocols. The scalability and security are addressed in the model.
[40]	2018	Consumer Security Index	The index methodology is addressed through four studies. The first one addressed the security features that should be provided for IoT devices. The second one employed a questionnaire to address the privacy features and preferences of disclosures while in study three, a matrix of IoT devices classes is developed. The fourth study the data extracted from user devices using natural language processing to find information about communication.
[41]	2017	Remote Security Management	The IoT devices security and safety is improved by a proposed architecture to handle the remote security management. Many cases of infringement was prevented and the damage was minimized.
[42]	2016	Security Configuration	The proposed on-demand technique for security configuration was deployed to configure the connected devices and reconfigure the new ones.
[43]	2019	Vulnerabilities Test	A structure of IoT is proposed to test the vulnerabilities of the devices in IoT environment. A hardware, software, and three test cases are testing the replication. The results are conducted after testing three test cases on smart thermostat and smart socket.
[44]	2015	Machine-To-Machine	The security issues related to machine to machine are considered. Many challenges and scams related to the financial billing system, communication mechanism, and protocol stacks are explained and listed.

VII. APPLICATIONS OF IOT

There are large number of applications could be innovated based on the integration between the IoT technology and the big data paradigm. This section explains the most important applications in this domain according to high score rate of the people thinking depends on Google, Twitter, and Linkedln reviews. The people think that the most important application of IoT-Big data is the health care applications [45]. The IoT-Big data can be deployed to conduct many health care applications such as track and monitor the health cases [46, 47], smart serving of health cases, and provide services related to bio medical. The researchers suggested the smart health care system such as monitor and track the health cases of "Dementia, Alzheimer's, Parkinson's and other problems" [45]. The IoT application can be applied through allow the sensors to produce alerts depend on the patients activities. The alerts would remember the patients about their medicines times, test dates, and other information related to the life of the patients. Hence, the daily life of the patients could be enhanced. Other important applications of the IoT-Big data are the smart city and the smart buildings. Using IoT technology the people and organizations can track and monitor the water, electricity, and telecommunication services. Thus, the provided services can be improved and the wasted resources can be reduced [48]. The public services can be monitored through electronic tags (sensors) that connected with the management offices in the city or buildings. Thus, the data can be collected from specific tags or all tags to produce electronic services such as the water amount that delivered for all/each house in the building or the city. The industry represents important implication of IoT-Big data [49]. Examples of industry applications are the intelligent transport through connect the vehicles (objects) with IoT network to track and monitor the transportation time, road traffic, and GPS. Also, the sensors can produce reports about the vehicles safety such as engine temperature and pressure of wheels. [49]. There are many other applications can benefits from the integration between the IoT technology and big data. Examples of these applications are the factory supply chains, the TV satellites, and people tracking in public areas. Table III lists a lists of literature works related to applications in the field of IoT based big data.

TABLE III
IOT APPLICATIONS BASED BIG DATA

Reference	Year	Domain	Aim of the Work
[50]	2019	Geo-Spatial Data	A proposed framework is developed to extract, sort, analyze, and process geospatial data efficiently. The outcomes of the project such as the platform architecture, future direction as well as current status are explained.
[51]	2018	Smart City	The researchers aim to enhance the smart city performance throughout using the IoT based on big data. The proposed a framework to beat the problem of big data with IoT by investigating the huge received information.
[52]	2019	Geo-Spatial Data	A geospatial dashboard for a city is proposed to collect, visualize and share the collected data from IoT devices and satellites. For improving planning process and spatial thinking in the field of disaster management, many geo-visualization tools of geo-spatial big data analysis are used.
[53]	2015	Road Traffic	Many IoT technologies are tested in the field of road traffic management such as timeline visualization tools to visualize the road traffic instantly based on traffic big data.
[54]	2018	Data Center Analysis	The model passed through three stages, the first stage showed the testing phase of the gigantic data using IoT devices. The second stage faced implementing tasks using Hadoop while a massive data analysis is performed in the third stage.
[55]	2019	Healthcare	A proposed framework of combining big data, IoT devices, and nano-electronics to enhance the ECG monitoring. The cost reduction, connectivity, and portability of ECG sensors are tested with big data IoT devices. The devices are tested in many fields to send data to different places such as cloud storage, doctor's end, and caregivers to analyze and process data.
[56]	2019	Home-Device	An analyzing framework of IoT big data devices is introduced to be used in the repair shop and smart home. The collected big data is analyzed at three different stages (distribution, customer usage, and A/S) stages. The framework can help in reducing distribution channel redundancy, and adjusting warehousing quantity. The framework consists of data crawler (to store and collect IoT home devices data), analyzer (to analyze big data), and visualization (to interpret the analytical results).
[57]	2018	Sentiment Analysis	The decision-oriented based sentiment analysis of big data and how it can be affected by IoT is discussed. Many related concepts to sentiment analysis in big data are introduced such as challenges, perspectives, decision value, features, and definitions. Many suggestions are concluded for the field of sentiment analysis in the field of IoT big data.
[58]	2017	Peripheral Control	Many storage devices are used for fast direct access for fetching, processing, analyzing the values of predefined data, and past data.
[59]	2019	Real-time Data Collection	The plugin of IoT is discussed as a solution for problems of the HPCC system where this system cannot handle the IoT applications and real-time IoT data for analyzing. This plugin can help in collecting real-time data for analyzing and supporting decision-making.
[60]	2019	Energy Consumption	A new subsystem for analyzing big data is proposed to suggest an effective solution for energy consumption based on machine learning and data analytics.
[61]	2014	Smart Industrial	For large automation applications in the industrial field, the implementation architecture framework of cognitive-oriented based IoT big data is proposed to manage data and discover knowledge effectively. The results showed that the framework creates practical solutions for smart applications in the field of industrial IoT big data.
[62]	2018	Vehicle Production	A model of common vehicle information is developed to allow representation, processing, and understanding chain. This model is a part of the project of exploiting the big data concept in building vehicles and using data of sensors. In the final stage, an evaluation process is implemented for the data of traffic measurement for all vehicles.
[63]	2019	Task Scheduling	A proposed approach for jobs and tasks scheduling in the field of big data is proposed to optimize tasks assignment for nodes. The results showed promising outcomes compared with the traditional scheduler.
[64]	2015	Environmental Protection	Many issues related to environmental protection based IoT big data such as management framework and features are outlined. Challenges, areas, characteristics of the applications in the field of IoT big data in China are listed.
[65]	2019	Data Analysis	An analysis framework of big data based apache of the crime sector is introduced. The framework collects the data set of problem-solving and keeps its secretiveness. The framework helps

			governments in decision-making related to policymakers and reduces crimes.
[66]	2017	Big Data Physical Objects	To overcome the problem of big data with software-defined networking, an architecture based IoT is proposed. The proposed solution based on analyzing the values of sensors in lower layers (gateway layer) before sending them out to the internet.
[67]	2019	Data Analysis	A proposed method for maintaining sensors optimal states is proposed in case the network fails due to big data intrusion or failure of sensors.
[67]	2017	Data Analysis	A framework of sensing agricultural data and collecting in cloud storage is proposed to analyze the cloud's big data for market, crops requirements, and stock requirements. A prediction approach using data mining algorithms is proposed and the farmer receives the prediction results via mobile application.
[68]	2016	Information Analysis	An optimal algorithm for efficient management of the data in the field of energy big data is produced after examining three algorithms in data analyzing.

VIII. CONCLUSION AND FUTURE WORKS

The IoT technology works on represent the life objects by electronic tags, connect the tags with each other, allow the data gathering with the objects, and processes the collected data to present meaningful service. The big data applications are happen as the connected IoT objects are increased. Thus, it is important to address the issues of IoT-Big data technology.

Thus, the IoT required to processes the objects communication using useful communication models and modes. The communication models need to transfer large amount of data of different structures in real time. Also, the data transfer need to be conducted in any time and from any place. Many researchers mentioned the importance of test the transfer protocols of IoT in order to decide the most suitable IoT structure for the big data applications. The IoT accomplished the data transfer and processing using several layers; coding layer, perception layer, network layer, middleware layer, application layer, and business layer. The big data transfer via the sequence of layer opens the opportunities for different attacking scenarios. Hence, it is important to adopt flexible and effective security approaches to protect the transfer data via IoT network.

There are many application could be innovated using IoT-big data technology and the people think that the health care applications are the most important. Other important applications are the smart city/building and the industrial applications like the intelligent transportation. According to [69], companies such as "UC Berkeley" and MIT were tested many IoT architectures to provide effective solutions for big data applications. The tests care about the requirements of big data applications such as the communication models, IoT protocols, and IoT security. However, this domain is still an issue for further development and enhancement. Many works could be conducted in the future to address challenges that face IoT-Big data. The tests could be conducted to judge the IoT performance for big data applications (i.e. effect of data amount on the IoT management and schedule the priority of data transfer via IoT, and analyze the workload of IoT based on various communication protocols). Other future works are related to the security of IoT for big data applications. The attacks scenarios could be analyzed based on different IoT layers and protocols in order to recommend effective security methods and approaches based on customized environments of big data.

REFERENCES

[1] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Transactions on industrial informatics, vol. 10, pp. 2233-2243, 2014.
[2] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in 2012 10th international conference on frontiers of information technology, 2012, pp. 257-260.
[3] K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview," The Internet Society (ISOC), vol. 80, 2015.
[4] C. S. YDB, "Terms of the Ubiquitous Network," 2011.
[5] I.-T. S. Y.2060, ""Overview of IoT"," 2012.
[6] E. Casagras, "Casagras final report: Rfid and the inclusive model for the internet of things," EU FP7 Project CASAGRAS, 2009.
[7] G. Lee and J. Park, "The IoT—Concept and Problem Statement," IETF Standard draft-lee-iot-problem-statement-05, 2012.
[8] Y. Ai, M. Peng, and K. Zhang, "Edge computing technologies for Internet of Things: a primer," Digital Communications and Networks, vol. 4, pp. 77-86, 2018.
[9] M. Li and X. Wang, "Delay and rate satisfaction for data transmission with application in wireless communications," IEEE Network, vol. 29, pp. 70-75, 2015.
[10] A. R. Mathew and A. Al Hajj, "Secure Communication on IoT and Big Data," Indian Journal of Science and Technology, vol. 10, 2017.
[11] I. A. Najm, A. K. Hamoud, J. Lloret, and I. Bosch, "Machine Learning Prediction Approach to Enhance Congestion Control in 5G IoT Environment," Electronics, vol. 8, p. 607, 2019.
[12] N. Elgendy and A. Elragal, "Big data analytics: a literature review paper," in Industrial Conference on Data Mining, 2014, pp. 214-227.
[13] C. Ji, Y. Li, W. Qiu, U. Awada, and K. Li, "Big data processing in cloud computing environments," in 2012 12th international symposium on pervasive systems, algorithms and networks, 2012, pp. 17-23.
[14] D. Rajeshwari, "State of the art of big data analytics: A survey," International Journal of Computer Applications, vol. 120, 2015.
[15] J. Nandimath, E. Banerjee, A. Patil, P. Kakade, S. Vaidya, and D. Chaturvedi, "Big data analysis using Apache Hadoop," in 2013 IEEE 14th International Conference on Information Reuse & Integration (IRI), 2013, pp. 700-703.
[16] I. A. T. Hashem, N. B. Anuar, A. Gani, I. Yaqoob, F. Xia, and S. U. Khan, "MapReduce: Review and open challenges," Scientometrics, vol. 109, pp. 389-422, 2016.
[17] S. Kulkarni and S. Kulkarni, "Communication models in internet of things: a survey," International Journal of Science Technology & Engineering, vol. 3, p. 3, 2017.
[18] U. N. Kar and D. K. Sanyal, "An overview of device-to-device communication in cellular networks," ICT express, vol. 4, pp. 203-208, 2018.
[19] B. N. Silva, M. Khan, and K. Han, "Internet of things: A comprehensive review of enabling technologies, architecture, and challenges," IETE Technical review, vol. 35, pp. 205-220, 2018.
[20] W. Chen, "An IBE-based security scheme on internet of things," in 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, 2012, pp. 1046-1049.

[21] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in 2012 international conference on computer science and electronics engineering, 2012, pp. 648-651.
[22] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of Internet of Things," in 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010, pp. V5-484-V5-487.
[23] M. Zhang, F. Sun, and X. Cheng, "Architecture of internet of things and its key technology integration based-on RFID," in 2012 Fifth International Symposium on Computational Intelligence and Design, 2012, pp. 294-297.
[24] M. U. Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A review on internet of things (IoT)," International Journal of Computer Applications, vol. 113, pp. 1-7, 2015.
[25] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE communications surveys & tutorials, vol. 17, pp. 2347-2376, 2015.
[26] Y. Zhang, "Technology framework of the Internet of Things and its application," in 2011 International Conference on Electrical and Control Engineering, 2011, pp. 4109-4112.
[27] P. Pavon-Marino and J.-L. Izquierdo-Zaragoza, "On the role of open-source optical network planning," in OFC 2014, 2014, pp. 1-3.
[28] C. Buratti, A. Stajkic, G. Gardasevic, S. Milardo, M. D. Abrignani, S. Mijovic, et al., "Testing protocols for the internet of things on the EuWIn platform," IEEE Internet of Things Journal, vol. 3, pp. 124-133, 2015.
[29] L. Lengyel, P. Ekler, T. Ujj, T. Balogh, and H. Charaf, "SensorHUB: An IoT driver framework for supporting sensor networks and data analysis," International Journal of Distributed Sensor Networks, vol. 11, p. 454379, 2015.
[30] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, 2005, pp. 46-57.
[31] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395-411, 2018.
[32] F. Olivier, G. Carlos, and N. Florent, "New security architecture for IoT network," Procedia Computer Science, vol. 52, pp. 1028-1033, 2015.
[33] H. Garg and M. Dave, "Securing IoT Devices and SecurelyConnecting the Dots Using REST API and Middleware," in 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 2019, pp. 1-6.
[34] J.-H. Han, Y. Jeon, and J. Kim, "Security considerations for secure and trustworthy smart home system in the IoT environment," in 2015 International Conference on Information and Communication Technology Convergence (ICTC), 2015, pp. 1116-1118.
[35] S. Pérez, J. A. Martínez, A. F. Skarmeta, M. Mateus, B. Almeida, and P. Maló, "ARMOUR: Large-scale experiments for IoT security & trust," in 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), 2016, pp. 553-558.
[36] J. Bugeja, B. Vogel, A. Jacobsson, and R. Varshney, "IoTSM: an end-to-end security model for IoT ecosystems," in 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2019, pp. 267-272.
[37] S.-R. Oh and Y.-G. Kim, "Development of IoT security component for interoperability," in 2017 13th International Computer Engineering Conference (ICENCO), 2017, pp. 41-44.
[38] P. L. R. Chze and K. S. Leong, "A secure multi-hop routing for IoT communication," in 2014 IEEE World forum on internet of things (WF-iot), 2014, pp. 428-432.
[39] N. Pazos, M. Müller, M. Aeberli, and N. Ouerhani, "ConnectOpen-automatic integration of IoT devices," in 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015, pp. 640-644.
[40] J. Blythe and S. Johnson, "The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices," 2018.
[41] S. Yoon and J. Kim, "Remote security management server for IoT devices," in 2017 International Conference on Information and Communication Technology Convergence (ICTC), 2017, pp. 1162-1164.
[42] B. Chung, J. Kim, and Y. Jeon, "On-demand security configuration for IoT devices," in 2016 International Conference on Information and Communication Technology Convergence (ICTC), 2016, pp. 1082-1084.
[43] M. Bettayeb, O. A. Waraga, M. A. Talib, Q. Nasir, and O. Einea, "IoT Testbed Security: Smart Socket and Smart Thermostat," in 2019 IEEE Conference on Application, Information and Network Security (AINS), 2019, pp. 18-23.
[44] K. Urunov, J.-I. Namgung, and S.-H. Park, "Security analysis based on Trusted Environment (TRE) of M2M/IoT," in 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), 2015, pp. 554-557.
[45] V. Vippalapalli and S. Ananthula, "Internet of things (IoT) based smart health care system," in 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), 2016, pp. 1229-1233.
[46] A. Humadi and A. Hamoud, "Online Real Time Fuzzy Inference System Based Human Health Monitoring and Medical Decision Making," International Journal of Computer Science and Information Security, vol. 15, pp. 197-204, 2017.
[47] H. N. H. Al-Hashimy, A. K. Hamoud, and F. A. Hussain, "The Effect of Not Using Internet of Things in Critical life Situations in the Health Field and the Effect on Iraqi Profitability: Empirical Study in Basra," Journal of Southwest Jiaotong University, vol. 54, 2019.
[48] J. Pan, R. Jain, S. Paul, T. Vu, A. Saifullah, and M. Sha, "An internet of things framework for smart energy in buildings: designs, prototype, and experiments," IEEE Internet of Things Journal, vol. 2, pp. 527-537, 2015.
[49] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," IEEE internet of things journal, vol. 1, pp. 289-299, 2014.
[50] J. Jo, I.-H. Joo, and K.-W. Lee, "Constructing National Geospatial Big Data Platform: Current Status and Future Direction," in 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), 2019, pp. 979-982.
[51] P. Yadav and S. Vishwakarma, "Application of Internet of Things and big data towards a smart city," in 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), 2018, pp. 1-5.
[52] K. K. Lwin, Y. Sekimoto, W. Takeuchi, and K. Zettsu, "City Geospatial Dashboard: IoT and Big Data Analytics for Geospatial Solutions Provider in Disaster Management," in 2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), 2019, pp. 1-4.
[53] A. Imawan and J. Kwon, "A timeline visualization system for road traffic big data," in 2015 IEEE International Conference on Big Data (Big Data), 2015, pp. 2928-2929.
[54] S. Lanka and S. Bajracharya, "Incorporating Big Data with IoT in Data Center Analytics," in 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT), 2018, pp. 240-245.
[55] M. Bansal and B. Gandhi, "IoT & Big Data in Smart Healthcare (ECG Monitoring)," in 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), 2019, pp. 390-396.
[56] J.-j. Jung, K. Kim, and J. Park, "Framework of Big data Analysis about IoT-Home-device for supporting a decision making an effective strategy about new product design," in 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), 2019, pp. 582-584.
[57] A. Dwivedi, R. Pant, S. Pandey, and K. Kumar, "Internet of Things'(IoT's) Impact on Decision Oriented Applications of Big Data Sentiment Analysis," in 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), 2018, pp. 1-10.
[58] M. S. Rani and B. Geetavani, "Design and analysis for improving reliability and accuracy of big-data based peripheral control through IoT," in 2017 International Conference on Trends in Electronics and Informatics (ICEI), 2017, pp. 749-753.

[59] K. A. Vardhan, M. Jakaraddi, G. Shobha, J. Shetty, A. Chala, and D. Camper, "Design and Development of IoT Plugin for HPCC Systems," in 2019 IEEE 4th International Conference on Big Data Analytics (ICBDA), 2019, pp. 158-162.

[60] E. Kassela, N. Provatas, A. Tsiourvas, I. Konstantinou, and N. Koziris, "BigOptiBase: Big Data Analytics for Base Station Energy Consumption Optimization," in 2019 IEEE International Conference on Big Data (Big Data), 2019, pp. 6098-6100.

[61] N. Mishra, C.-C. Lin, and H.-T. Chang, "A cognitive oriented framework for IoT big-data management prospective," in 2014 IEEE International Conference on Communiction Problem-solving, 2014, pp. 124-127.

[62] J. Pillmann, B. Sliwa, and C. Wietfeld, "The AutoMat CVIM-A Scalable Data Model for Automotive Big Data Marketplaces," in 2018 19th IEEE International Conference on Mobile Data Management (MDM), 2018, pp. 284-285.

[63] K. Hadjar and A. Jedidi, "A New Approach for Scheduling Tasks and/or Jobs in Big Data Cluster," in 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC), 2019, pp. 1-4.

[64] S. Q. Lu, G. Xie, Z. Chen, and X. Han, "The management of application of big data in internet of thing in environmental protection in China," in 2015 IEEE First International Conference on Big Data Computing Service and Applications, 2015, pp. 218-222.

[65] A. Bhat, "An analysis of Crime data under Apache Pig on Big Data," in 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2019, pp. 330-335.

[66] M. T. Kakiz, E. Öztürk, and T. Çavdar, "A novel SDN-based IoT architecture for big data," in 2017 International Artificial Intelligence and Data Processing Symposium (IDAP), 2017, pp. 1-5.

[67] S. Seo and J.-M. Chung, "Outlier Detection Technique for IoT Sensor-Driven Big Data Systems," in 2019 International Conference on Electronics, Information, and Communication (ICEIC), 2019, pp. 1-2.

[68] D. Kang, S. Kim, T. Lee, J. Hwang, S. Lee, S. Jang, et al., "Energy information analysis using data algorithms based on big data platform," in 2016 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 (HPCC/SmartCity/DSS), 2016, pp. 1530-1531.

[69] H. Fang, Z. Zhang, C. J. Wang, M. Daneshmand, C. Wang, and H. Wang, "A survey of big data research," IEEE network, vol. 29, pp. 6-9, 2015.