EasyChair Preprint

№ 4135

A Survey on Remote Diagnostic of Campus Network using IoT devices

Akangkhi Borah and Bobby Sharma

September 3, 2020

A Survey on Remote Diagnostic of Campus Network using IoT devices

Akangkhi Borah and Dr Bobby Sharma
Department of CSE, School of Technology
Assam Don Bosco University, Azara
Guwahati, India-781017
Email: borah.akangkhi@gmail.com

***Abstract*— the future home, workspace, campus or city, as predicted by science fiction in early times is now a reality. Modern microelectronics and communication technologies offer the type of smart living that looked practically inconceivable just a few decades ago. The internet of Things (IoT) is one of the main drivers of the future smart spaces. IoT refers to the networking of physical objects which contains sensors and software that allow objects to exchange data. It enables new operational technologies and offers vital financial and environmental benefits. With IoT, spaces are evolving from being just smart to become intelligent and committed. This survey paper focuses on how to leverage IoT technologies to build a modular approach to smart campuses. This paper identifies the key benefits and motivation behind the development of IoT-enabled campus. Then it provides a comprehensive view of general types of smart campus application. Finally we considered the vital design challenges, which should be met to realize the smart campus.**

Keywords- Smart Campus, IoT devices, IoT Network Sensors, Wireless Sensor Networks, Smart homes, Smart grids, Network anomalies, Arduino, ESP8266.

I. INTRODUCTION

Internet of Things is the integration of physical objects which are attached with electronics, software, sensors, and network connectivity between then, that allow them to capture and transmit data [1]. In IoT, a thing refers to a physical object that include sensors to communicate with the real world through a network to perform certain functions. IoT devices may from a network system which links various communication devices to have quick, reliable and real-time information exchange and communication that would help in intelligent management of the connected devices. As a result, objects can be monitored and managed remotely allowing for the communication between the physical and virtual worlds [2, 3].

With the advanced on computing and wireless communication technologies, emerging and exciting Internet of Things network, more cities and university campuses are becoming smart, meaning that they are implementing those technologies to exchange data [4]. The objective of being smart is to simplify the administration process, manage real-time access control, monitor the constraints, and so on [5].

Smart campuses has the potential to revolutionize the education and maintenance system and offer the capability to enhance the campus operating effectiveness, while delivering high quality service to the campus community [6-8]. It provides an interactive and creative environment for students, faculty, staff, and management. Institutes or campuses focuses on improving the quality of service by providing a way to share resources, knowledge content, and exchange of skills. All the IT resources and content should be available to the public or users in the campus from their desk as well as anywhere-anytime basis over the campus. To achieve the same, the institute/organization needs to establish campus networks on their campuses. It is very helpful for the institution to work from any building and receive the same speed of data transfer. A typical campus network or campus area network is a computer network made up of an interconnection of local area networks (LANs) within a limited geographical area that may interconnect administrative buildings, residence halls, academic buildings, libraries, student centers, athletic facilities and other building associated with the institution in the case of a college or university campus network [9-13]. The networking equipment (switches, routers, firewalls) and transmission media (optical fiber, twisted copper pair) are use to interconnect and communicate among all connected device. Deploying IoT devices for remote monitoring and management of networking devices in a campus network would ensure automated remote diagnostics and maintenance, thus providing early warnings for faulty network equipment, and ensure easy repairs without interrupting the normal work process.

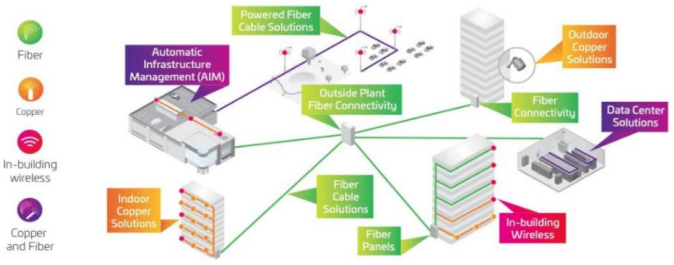

fig.1: Connected Campus Infrastructure

In the late 1960's and early 1970's, the techniques for remote monitoring of computer system were beginning to be explored, many of them were based on existing hardware and software technologies. Some classification of remote monitors which are as follows [14]: -

- Remotely controlled software monitors
- Computer network monitors
- Fault diagnosis monitors
- Intelligent and extended consoled

The rest of the paper has been organized in following sections: Section II explains the background of Internet of Things, and the technologies associated with it. The IoT network architecture is mentioned in Section III of the paper. The major concerns over the application of IoT is pictured in Section IV. Finally, a conclusion has been formulated in Section V, which leads to end of this survey report.

II. NETWORK TERMINOLOGIES

A. *Wireless Sensor Network*

Wireless Sensor Network (WSN) is a network that consists of sensor nodes with an embedded processor [15]. The sensor nodes usually are spatially distributed to monitor physical or environmental conditions, such as humidity and temperature. They work cooperatively and pass their data through the network to a center location. When visual sensor (camera) is included, the network is referred to visual sensor network, which capable of processing images into a more useful form [16]. With the use of camera in sensor network, one can create important applications, such as video surveillance, which sometimes includes algorithm like object tracking.

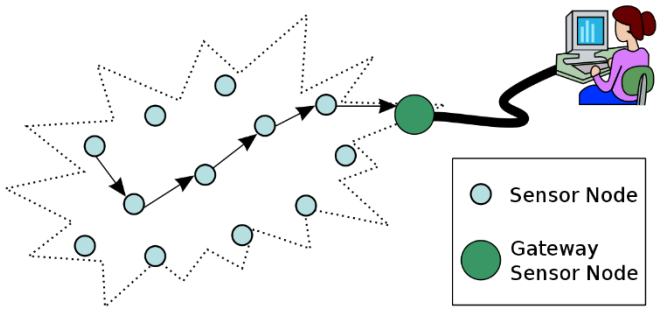

fig.2: Wireless Sensor Network (WSN)

B. *Internet of Things*

The phrase "Internet of Things" was coined in 1999 by Kevin Ashton, to represent the concept of computers and machines with sensors, that connected to the internet [17]. Initially, the network was based on Radio Frequency ID (RFID) chips. After popularized by MIT, the IoT application grows into many different fields, such as surveillance, security, transportation, smart cities, etc. [18].

In Internet of Things, there are connectivity between computers and other physical devices such as network devices, buildings and automobiles, embedded with sensors and network connectivity that enable the reading from sensors and actuators to be monitored from the internet or intranet. IoT connects wireless sensor network (WSN) to Internet, where the sensor nodes in WSN are regard as the "things" in IoT [19]. The IoT also allows objects to be controlled remotely and becomes the base of technologies such as smart cities and smart homes [20].

Any devices integrated into the Internet of Things are having the following characteristics [21]: -

- The devices are located in an environment to be monitored, which has the capabilities of sending data to the internet or to other devices.
- The devices are programmable to act accordingly.
- The device is part of a collection of devices that can communicate with each other through other nodes in the same network.

C. *Arduino*

Arduino is an easy-to-use hardware and software based on open-source prototyping platform [25]. Originally, Arduino was created as tool for fast prototyping, aimed for students without any background in electronics and programming. Later, the Arduino board started to change to adapt to new needs and challenges. All Arduino boards (and software) are completely open-source. There are different versions of Arduino available on the market (UNO, Mega, Mini, Yún, etc.). Arduino uses power from computer (by USB cable), AC to DC adapter, or batteries. Arduino can extend communication via Ethernet, WiFi, GPRS, and GSM by using shields. Shields have the same pin location as the Arduino, so it is easy to assembly with [26].

fig.4: Arduino UNO with Ethernet Shield

D. *ESP8266 Wi-Fi Module*

The ESP8266 Wi-Fi module is a self-contained system on a single chip with integrated TCP/IP protocol stack and microcontroller capability. It can be connected to Arduino to give it Wi-Fi access, as a Wi-Fi shield offer. This module has on-board processing power and storage capability to be integrated with sensors and other application specific devices through General Purpose Input Output (GPIO). A self-calibrated RF allows it to work under any operating conditions, without any external RF parts [27].

fig.5: ESP8266 with on-board Wi-Fi antenna

The ESP8266 is a cost effective module with increasing community, with following features [27]: -

- 802.11 b/g/n with Integrated TCP/IP protocol
- 80 MHz 32-bit microcontroller
- 4 MB Flash Memory
- Wake up and transmit packets in less than 2ms
- Standby power consumption of less than 1.0mW

The ESP8266 Wi-Fi module works like an Arduino and can also be used with Arduino as the communication module.

III. Related Works

A. *Smart Homes and Buildings*

With the recent advances in IoT technologies, the smart home and smart building concept has evolved enormously. Smart homes incorporates common devices that control features of the home. Originally, smart home technology was used to control environmental systems such as lighting and heating but recently the use of smart technology has developed so that almost any electrical components within the house can be included in the system [22, 23]. Moreover, smart home technology does not simply turn devices on and off, it can monitor the internal environment and the activities that are being undertaken whilst the house is occupied. The result of this modification to the technology is that a smart home can now monitor the activities of the occupant of a home, independently operate devices in set of predefined patterns and as the user requires [24].

fig.3: Smart Homes and Buildings

B. *IoT in campus application*

The IoT refers to intelligently connected devices and systems to gather data from embedded sensors and actuators and other physical objects. IoT is expected to spread rapidly in the coming years a new dimension of services that improve the quality of campus infrastructure and easy to function for students and whole admin staffs including professors.

In every organization or institution, there is always an information desk that provides information, advertisement messages and many notifications to their customers and staff. The problem is that it requires some staff that is dedicated to that purpose and that must have up to date information about the offers advertisement and the organization. Due to IoT, we can see many smart devices around us. Many people hold the view that cities and the world itself will be overlaid with sensing and actuation, many embedded in “things” creating what is referred to as a smart world. Similar work has been already done by many people around the world. This time mobile networks already deliver connectivity to a broad range of devices, which can enable the development of new services and applications. This new wave of connectivity is going beyond tablets and laptops; to connected cars and buildings; smart meters and traffic control; with the prospect of intelligently connecting almost everything and anyone also includes troubleshooting.

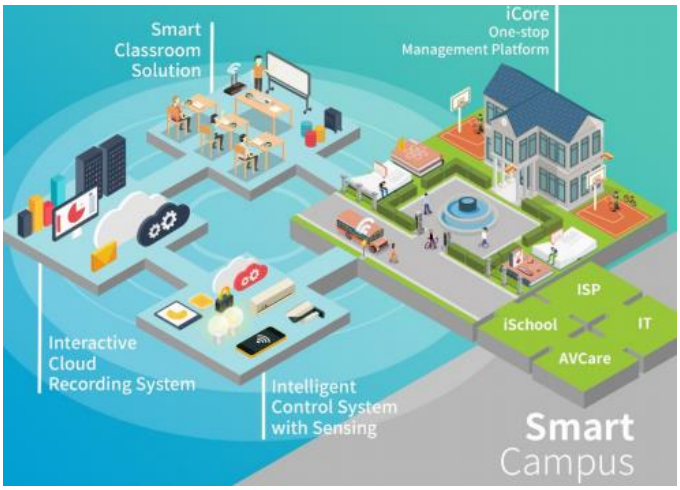

fig.3: Simulation os a connected smart campus

C. *Remote diagnostics using IoT*

With Remote diagnostics is the act of diagnosing a given symptom, issue or problem from a distance. Instead of the subject being co-located with the person or system has done diagnostics, with remote diagnostics the subjects can be separated by physical distance. Important information is exchanged either through wired or wireless. When limiting to systems, a generally accepted definition is: “To improve the reliability of vital or capital-intensive installations and reduce the maintenance costs by avoiding unplanned maintenance, by monitoring the condition of the system remotely.”

In all likelihood, remote diagnostics and management will be a combination of automated and semi-automated capabilities that are supplied by multiple, coordinated parts of the IoT service. For instance, different capabilities will need to come

from different service providers to effectively discover and trace problems.

IV. NETWORK ARCHITRECTURE

The IoT devices generates a huge amount of tiny information, which needs media to get stored [28]. Real world objects are the main components of the IoT paradigm, each object has a unique identity and can access the network to integrate the physical and digital world to offer enhanced capabilities to people. The IoT devices needs to be connected over a network to upload data to a server, wherein the data will be processed, stored and displayed. The IoT device can offer device to device, device to people and device to environment information transmission through the incorporation of information space and physical space. Many different network architectures has been practiced for data uplink from the devices to application servers. Some of the network topologies are mentioned as follows [29]:-

A. Point-to-point (P2P) Topology

Point-to-point wireless network can be used to connect two distant IoT devices together and can form a network. It is also called a P2P link. The name describes the concept: two points are connected together, and nothing else. This requires two wireless capable devices. One device may work as the sensor node and the other device as the gateway node to receive the data from the sensor node and forward it to the application server [30, 31].

fig.6: ESP8266 in P2P topology

The above network comprises of two ESP8266, one in STA and other in AP mode connected though each other. The node in STA mode is the sensor node generating data from the environment with the help of sensors and the node in AP mode is the gateway node gathering data from the sensor node for processing, storage and visualization.

B. Star Network Topology

A Star network consist of one central hub (a.k.a. gateway node), to which all the other nodes (e.g. the sensor nodes) in the network are linked. This central hub acts as a common connection point for all the other nodes in the network. All peripheral nodes may thus communicate with all others by transmitting to, and receiving from, the central hub only. The performance of the network is consistent, predictable and fast (low latency and high throughput) [32, 33].

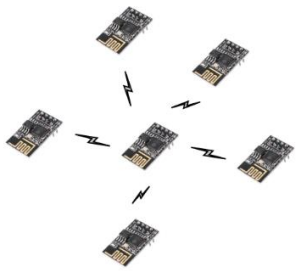

fig.7: ESP8266 in Star Network Topology

In a star network, a data packet typically travels one hop to reach its destination yielding a very low and predictable network latency. Also, there is high overall network reliability due to the ease with which faults and devices can be isolated. Each device, utilizes its own single link to the hub. This makes the isolation of individual devices straightforward and makes it easy to detect faults and to remove failing components [34-36].

In fig. 7; Multiple ESP8266 is connected to form an IoT network wherein one ESP8266 is working as gateway node and the other ESP8266 are working as sensor nodes. The data generated by the sensor nodes are transmitted to the gateway node with only one hop from source to destination.

C. Mesh Network Topology

A mesh network consist of three different types of nodes, a gateway node as in a star node, simple sensor nodes and sensor nodes with repeater/routing capability. Mesh network nodes are deployed such that every node is within transmission range of at least one other sensor node. Data packets pass through multiple sensor nodes to reach the gateway node. This networking topology is used for many application requiring a long range and broad area coverage. Mesh network can scale up to thousands of nodes, providing a high density of coverage with a broad assortments of sensors and actuating devices. Data can be transmitted from different nodes simultaneously. This topology can withstand high amount of traffic. Even if one of the node fails, there is always an alternative present. So data transfer doesn't get affected, and expansion and modification in topology can be done without disrupting other nodes [37].

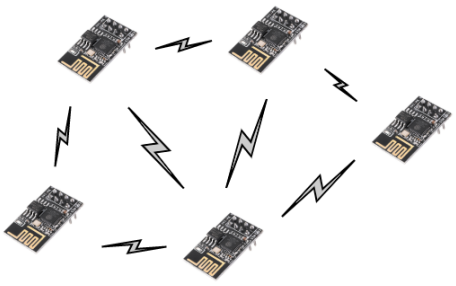

fig.8: ESP8266 in Mesh Network Topology

The above network is made up of multiple ESP8266 acting as sensor nodes with repeater/routing capabilities, with one

ESP8266 acting as gateway. The data generated by the sensors connected to the ESP8266 are transmitted to the gateway node with generally one or more hop from the source to destination. This helps in expanding the sensor network and can support lots of devices with redundancy in data transmission.

V. CONCERNS OVER IOT

The Internet of Things is a modern era technology but the challenges and issues concerning to IoT are enormous. Numerous consideration are need to be done before implementing IoT in different applications. Some of the issues are as follows [38];

A. Design Issues

Designing a simple computer network involves many consideration from hardware components to the software version incorporated for the same. So, for designing an IoT network system would need numerous design consideration [39].

B. Security Issues

As we know, no computer system is fully secured from security threats. With up to 50 billion devices to be connected to the internet by 2020, security threats needs to be addresses. Data integrity and compatibility issues would topple economics across the global market if not defended. For example, jamming of radio networks in a hospital that uses smart wireless environment could be disastrous. These kinds' drawbacks could delay the deployment progress of IoT [40].

C. Hardware Issues

In order to setup a full-fledged IoT network, there are various hardware elements to be made use of, such as sensors, development boards, gateways, and much more. Hence, enterprises need to make sure that they source their hardware from the same manufacturer to avoid compatibility issues. IoT devices are manufactured to target customers with a very low price tag, this leads to compromises in quality of these IoT devices. Industrial grade IoT devices are manufactured to withstand high temperatures and have high environmental tolerances, but they come with a price. Also, most IoT devices are portable and battery powered. So, their hardware design must be optimized to work with low current for longer operation on battery. These are some of the hardware issues found on IoT devices which are hampering the growth of IoT in the industrial field [41].

VI. CONCLUSION

In this survey paper, we investigated the recent work of using IoT on smart campus from different perspective including smart homes and buildings and the IoT hardware associated with it with the various issues faced by it. Due to the rapid advances in technology and industrial infrastructure, IoT is expected to be widely applied to industries. Industries have strong interest in deploying IoT devices to develop industrial application such as automated monitoring, control, management, and maintenance. A smart campus can be realized using an IoT-enabled computing environments to establish an infrastructure for the application to create and deliver value added services. In addition, we give insights on the concerns, which decelerates the smart campus from becoming reality.

REFERENCES

[1] Abuarqoub, Abdelrahman & Abusaimeh, Hesham & Hammoudeh, Mohammad & Uliyan, Maas & Abu-Hashem, Muhannad & Murad, Sharefa & Al-Jarrah, Mudhafar & Alfayez, Fayez. (2017). A Survey on Internet of Things Enabled Smart Campus Applications. 1-7. 10.1145/3102304.3109810.

[2] Sreekar, Siddula & Bobba, Phaneendra & Jain, Prem. (2018). Water Level Monitoring and Management of Dams using IoT. 1-5. 10.1109/IoT-SIU.2018.8519843.

[3] S. Marstijepović and S. Williams, "Environmental monitoring and field surveillance reference guide.pdf." [Online]. Available: http://www.undp.org/content/dam/montenegro/docs/publications/ee/WBEPandENVSEC/Environmental monitoring and field surveillance reference guide.pdf.

[4] Gahlaut, Swati & Seeja, K.R. (2017). IoT based smart campus. 1-4. 10.1109/ICICCIS.2017.8660956.

[5] Juhari, Muhammad & Mansor, H.. (2016). IIUM Bus on Campus Monitoring System. 138-143. 10.1109/ICCCE.2016.40.

[6] Sánchez, A.s & Esquerre, Karla. (2018). Internet of Things for a Smart Campus On Line Monitoring of Water Consumption in University Buildings. International Journal of Engineering and Technical Research. 7. 10.17577/IJERTV7IS030187.

[7] Kar, Arpan & Gupta, MP. (2015). How to make a Smart Campus - Smart Campus Programme in IIT Delhi. 10.13140/RG.2.1.4629.9601.

[8] Widya Sari, Marti & Wahyu Ciptadi, Prahenusa & Hardyanto, R.. (2017). Study of Smart Campus Development Using Internet of Things Technology. IOP Conference Series: Materials Science and Engineering. 190. 012032. 10.1088/1757-899X/190/1/012032.

[9] Yu, Minlan & Rexford, Jennifer & Sun, Xin & Rao, Sanjay & Feamster, Nick. (2011). A Survey of Virtual LAN Usage in Campus Networks. Communications Magazine, IEEE. 49. 98 - 103. 10.1109/MCOM.2011.5936161.

[10] Kumari, Lalita & Debbarma, Swapan & Shyam, Radhey. (2011). Security Problems in Campus Network and Its Solutions. International Journal of Advanced Engineering & Applications (IJAEA). Volume-1. pp 98-101.

[11] Ali, Md. Nadir & Rahman, M. & Hossain, Syed. (2013). Network architecture and security issues in campus networks. 1-9. 10.1109/ICCCNT.2013.6726595.

[12] Ullah, Zaka & Hasan, Muhammad Zulkifl. (2017). Implementation challenges in Campus Network security.

[13] Ali, Md. Nadir. (2015). Design and Implementation of a Secure Campus Network. Journal of Surface Engineered Materials and Advanced Technology. 5.

[14] Gary J. Nutt, Ph. D., "A Survey of Remote Monitoring". Institute of Computer Scienc and Technology, National Bureau of Standards, Washington, D.C.

[15] N. P. Sastra and G. Hendrantoro, "Energy Efficiency of Image Transmission in Embedded Linux based Wireless Visual Sensor Network.," Journal of Communications Software & Systems, vol. 11, no. 3, 2015.

[16] D. M. Wiharta, Wirawan, and G. Hendrantoro, "On the Accuracy of Particle Filter-Based Object Tracking," International Journal of Multimedia and Ubiquitous Engineering, vol. 10, no. 11, pp. 265–276, 2015.

[17] D. Palma, J. E. Agudo, H. Sancez, and M. M. Macias, "An Internet of Things Example: Classrooms Access Control over Near Field Communication," Sensors, vol. 14, no. 4, 2014

[18] K.-D. Chang and J.-L. Chen, "A survey of Trust Management in WSNs,Internet of Things and Future Internet.," KSII Transactions on Internet and Information Systems, vol. 6, no. 1, pp. 5–23, 2012.

[19] Rawat, Priyanka & Singh, Kamal & Chaouchi, Hakima & Bonnin, Jean-Marie. (2013). Wireless sensor networks: A survey on recent

developments and potential synergies. The Journal of Supercomputing. 68. 10.1007/s11227-013-1021-9.

[20] Klein, Cornel & Kaefer, Gerald. (2008). From Smart Homes to Smart Cities: Opportunities and Challenges from an Industrial Perspective. 260. 10.1007/978-3-540-85500-2_24.

[21] Patel, Keyur & Patel, Sunil & Scholar, P & Salazar, Carlos. (2016). Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges.

[22] Madakam, Somayya. (2014). Smart Homes (Conceptual Views). 10.1109/ISCBI.2014.21.

[23] Totonchi, Ahmed. (2018). Smart Buildings Based On Internet Of Things: A Systematic Review.

[24] Bouchard, Kévin & Bergeron, Frédéric & Giroux, Sylvain. (2017). Applying Data Mining in Smart Home. 10.1201/9781315145686-7.

[25] "Arduino - Home." [Online]. Available: https://www.arduino.cc/.

[26] "WiFi Module - ESP8266 - WRL-13678 - SparkFun Electronics." [Online]. Available: https://www.sparkfun.com/products/13678.

[27] Bhatti, Emmy & Sharma, Sonia. (2017). Big IoT Data Analysis: A Generic Overview. www.ijcst.com.

[28] Dhanvijay, Mrinai & Patil, Shailaja. (2019). Internet of Things: A Survey of Enabling Technologies in Healthcare and its Applications. Computer Networks. 153. 10.1016/j.comnet.2019.03.006.

[29] Adiono, Trio & Fuada, Syifaul & Luthfi, Muhamad & Saputro, Rosmianto. (2017). MAC Layer Design for Network-Enabled Visible Light Communication Systems Compliant with IEEE 802.15.7. EAI Endorsed Transactions on Energy Web. 4. 153163. 10.4108/eai.4-10-2017.153163.

[30] Chang, Chih-Yung & Kuo, Chin-Hwa & Chen, Jian-Cheng & Wang, Tzu-Chia. (2015). Design and Implementation of an IoT Access Point for Smart Home. Applied Sciences. 1882-1903. 10.3390/app5041882.

[31] Silva, Pedro & Kaseva, Ville & Lohan, Elena Simona. (2018). Wireless Positioning in IoT: A Look at Current and Future Trends. Sensors. 18. 2470. 10.3390/s18082470.

[32] Marin, Leandro & Pawlowski, Marcin & Jara, Antonio J.. (2015). Optimized ECC Implementation for Secure Communication between Heterogeneous IoT Devices. Sensors (Basel, Switzerland). 15. 21478-21499. 10.3390/s150921478.

[33] Invidia, Lorenzo & Oliva, Silvio & Palmieri, Andrea & Patrono, Luigi & Rametta, Piercosimo. (2019). An IoT-oriented Fast Prototyping Platform for BLE-based Star Topology Networks. Journal of Communications Software and Systems. 15. 10.24138/jcomss.v15i2.682.

[34] Mekki, Kais & Bajic, Eddy & Chaxel, Frédéric & Meyer, Fernand. (2018). Overview of Cellular LPWAN Technologies for IoT Deployment: Sigfox, LoRaWAN, and NB-IoT. 10.1109/PERCOMW.2018.8480255.

[35] Gutiérrez, Daniel & Toral, S.L. & Barrero, Federico & Bessis, Nik & Asimakopoulou, Eleana. (2013). The Role of Ad Hoc Networks in the Internet of Things: A Case Scenario for Smart Environments. 10.1007/978-3-642-34952-2_4.

[36] Liu, Yu & Tong, Kin-Fai & Qiu, Xiangdong & Liu, Ying & Ding, Xuyang. (2017). Wireless Mesh Networks in IoT Networks. 183-185. 10.1109/iWEM.2017.7968828.

[37] Yadav, Er Pooja & Yadav, Hemant. (2018). IoT: Challenges and Issues in Indian Perspective. 10.1109/IoT-SIU.2018.8519869.

[38] Gardasevic, Gordana & Veletić, Mladen & Maletic, Nebojsa & Vasiljevic, Dragan & Radusinovic, Igor & Tomovic, Slavica & Radonjic, Milutin. (2017). The IoT Architectural Framework, Design Issues and Application Domains. Wireless Personal Communications. 127-148. 10.1007/s11277-016-3842-3.

[39] Xu, Teng & Wendt, James & Potkonjak, Miodrag. (2014). Security of IoT Systems: Design Challenges and Opportunities. IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers, ICCAD. 2015. 10.1109/ICCAD.2014.7001385.

[40] Koley, Subha & Ghosal, Prasun. (2015). Addressing Hardware Security Challenges in Internet of Things: Recent Trends and Possible Solutions. 10.1109/UIC-ATC-ScalCom-CBDCom-IoP.2015.