Practical application of IOT and its implications on the existing software

Israa Al_Barazanchi
Baghdad College of Economic Sciences University - Baghdad, Iraq, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.
israa44444@gmail.com

Zahraa A. Jaaz
College of Science - Computer department – Al-Nahrain University, Baghdad,
zaj@sc.nahrainuniv.edu.iq

Haider Hadi Abbas
Computer Technology Engineering Department, Al-Mansour University College (MUC), Iraq,
haider.hadi@muc.edu.iq

Haider Rasheed Abdulshaheed
Baghdad College of Economic Sciences University - Baghdad, Iraq, Faculty of information and communication technology, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.
haider252004@yahoo.com

***Abstract*—The data management from end-to-end level is done by cloud-assisted IOT for its users and they keep a goal in increasing their number of users with the course of time. From saving the infiltration of data from both internal and external threats to the system, IOT is the best-proposed method used for securing the database. Connecting objects/individuals with the Internet via safe interaction is the main objective of IOT. It can assemble all the hardware devices that are designed to store data for an individual or an organization. The associated applications and the way in which it can be deployed in the present organization in order to optimize the current working system. This paper focuses on providing an overall systematic secured data sharing portal that is devoid of threats from internal as well as external entities. By using CIBPRE data encryption a major security reform is introduced by IOT in storing and sharing of data on a regular basis.**

***Keywords*— IOT, Cloud computing, wireless technology,3-layer architecture**

I. INTRODUCTION

When data is stored in the cloud, it is posted in a scattered format that is not easily accessible by the users [1]. Also, finding data on the cloud might reveal those data that are posted by other parties and confidentiality of data uploaded is not maintained [2]. Whereas in planning a framework for IOT, this problem can be approached in a different way and solutions can be obtained. To meet the ends of security measures asked by fellow clients, the framework is designed accordingly [3]. Meeting the security needs of the concerned client with the flexible timeframe of security given by IOT is quite difficult. It cannot be reformed within the given time span and be adaptable for the clients. To consummately settle such high-security grounds, one needs to work on it for a long period of time [4]. Generally, trust dependent security layers are introduced in the system. But even they don't have enough means to cater to the needs of an individual. In the same manner, IOT cannot give solutions to storing data anonymously and keep muddling the data [5]. This ensures that unlike cloud that simply stores data without security measures, IOT is responsible for securing the data in the first phase and then only proceed on another forum. Cloud becomes a memory closet without any sort of arrangement while IOT proves to manage the stored data by dynamic solutions in accessing the data [6]. The figure 1. Shows the IOT system and its connectivity.

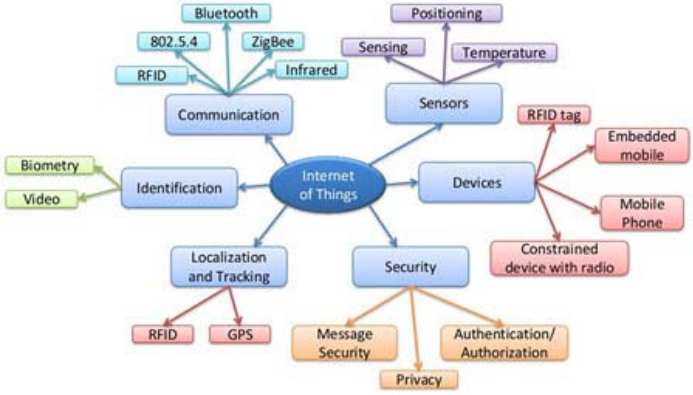

Figure 1: the IOT system and its connectivity [21]

Several cryptographic strategies are used to keep the confidentiality of the data intact and not reveal it to random users [6]. By expanding IOT with cloud, several security models have to be altered in order to check potential assailants categorically in the primary state [7]. The secondary state is to make sure that the effects of the adaptability of IOT are not imposing problems on security reforms. It is advised to use CIBPRE abbreviation of Contingent Personality Based Communicate Intermediary Re-encryption for accessing the security models built for intermediary re-encryption conspiracy. These modern techniques give a promising platform to provide security measures by encoding the data and storing it in an encrypted format. This can only be deciphered by the end-user eligible to access the encrypted data [8]. With an increasing number of clients joining IOT, the cloud capacity needs to increase, so that maximum data can be stored.

II. BACKGROUND STUDY

Connecting the internet with the appliances have come in trend ce the past decade. But they were discussed back in 1982 [9]. A modified version of the vending machine was introduced at Carnegie Mellon University and it was the first object that got linked with the internet. It kept a track of the drinks that were served and showed whether the drinks were hot or cold. As time passed, in 1991 Mark Weiser started that it is important to connect the con ers of the 21st century to the objects used in our daily life [10]. The interconnection of

devices, machines, objects, mechanical appliances, and humans through the internet with the ability to transfer and storing of data without any interaction of human-to-computer is the goal of IOT. It is an integration of wireless communication, systems that are correlated at a micro-level with electronics and mechanical engineering, services at the micro-level and internet

The protocol set for using IOT is, collecting data, optimization of data, storing it on the defined portal, and lastly channeling it with the internet. The above process seems to be easy but when followed in a systematic manner with high control security measures, it sure serves to be the most comprehensive solution for all your data storing needs [11]. Technologies that have committed themselves to IOT are divided into two parts: Wired technology and Wireless Internet Access.

A. Assigning an address to specific objects

This system strives to create an electronically generated product code to be assigned to an individual object. This Auto-ID concept is originally related to RFID-tags. Every object is given a unique IP address or a predefined URI that is stored in the system. Rather than using individual names for the products, a system-generated code is assigned in the form of URI. These codes are stored in the central server and form a systematic format for their human users . Users don't have to remember URI for each object. When the particular object is referred, the object itself won't converse directly to the user and its IP address would be referred instead as the specific identifier [10]. The IP generating software is evolving with a greater number of objects assigned on the Internet via IOT format. Initially, IPv4 was used to assign addresses to objects linked with the internet. Now, IPv6 is used to assign larger addresses with more specifications and a higher level of encrypted format.

B. Wireless technology

Short-range frequency:

Under this range, data collection is done within an assigned area. The designated area can be defined in terms of kilometers, a number of users, or any such thing [12].

Mesh networking: this type of networking is used when sharing of data takes place within a short-range. It is Bluetooth low energy technology which has a larger number of users in a confined application platform.

Light-Fidelity: this works in the visible region with increased bandwidth to provide better data transferring solutions. It is similar to Wi-fi, Figure 2: Shows NFC Technology.

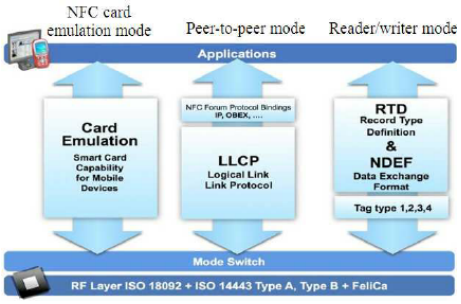

Figure 2: NFC Technology [24]

Near Field Communication: in this protocol, electronic devices are communicating within fewer than 4 cm.

ZigBee: it works on the platform of the personal area network where files are transferred with higher security measures and at a lower rate of power consumption with slow data transfer.

Z-Wave technology: this type of communication of data transfer is generally used in upgrading home automation and security systems.

Radio Frequency Communication: RFID: This type of assigning protocol works on radio frequency in electromagnetic fields.

Wi-Fi: the local area networking concept of using Wi-Fi technology comes with a benefit where users using a local network can transfer files over Wi-Fi remotely without any problem between two individuals [13].

Medium Range Frequency:

The name itself suggests that data transfer occurs over an area that is larger than that of smaller frequency regions.

An advanced version of LTE: this type of data transfer protocol is strongly recommended for mobile transmissions. They have increased their standards by providing a platform for data transfer with extended coverage and low latency measures with a higher throughput level.

Long-range Frequency:

Wide area network:

This allows data transfer over a long-range for communication of devices. The rate of transmission and power consumption is reduced resulting in slow transfers over large distances. Very Small Aperture Terminal: this technology is used to transfer data over large distances using dish antennas. Both broadband and narrowband data transmission are acquired through this. It is mainly used for satellite communications.

C. Wired technology

This technology is used for data transfer and storing of data between devices that are physically connected through wires and cables. It is a network built with hardware wires and fiber optics to carry data in their channel and transmit from one device to another [14]. The two modes for communicating in a wired manner are:

- Ethernet
- PLC: Power Line Communication

Using these technologies in primary or secondary format, few standards are set by IOT to collect data over the internet and keep it secured.

The technical standards involved are [15]:

- Auto-ID: Auto Identification Center that works on RFID technology
- EPCglobal: Electronic product code technology
- FDA: mainly used by medical devices for unique device identification
- GS1: used for consumer goods that need to be addressed for a fast movement like health care supplies
- IEEE: the standard form for communication under the Institute of Electrical and Electronics Engineers
- IETF: follows internet protocol comprising TCP/IP

- MT connect institute: mainly defined for data exchange within machines and other industrial equipment
- O-DF: Open data format is assigned in 2014 specifically for the general information of the model structure to define the 'thing' in IOT for updating data and publishing it on online platforms
- O-MI: Open Messaging Interface mainly works for limited objects that are performing key operations for a different type of subscribed mechanism
- OCF: open connectivity foundation mainly used for simple data transfer
- OMA: open mobile alliance is mainly used for providing high-security reforms for IOT standards
- XSF: extensible messaging and presence protocol mainly used for sharing instant messages on runtime format.

III. IOT Organization

The Internet of things has attracted most of the organizations in changing their present system of assigning data and storing it to their hard drives to IOT technology. Here networking of objects in use can be done from remote access and the connectivity is granted to a group of predetermined people in accessing the stored data. Implementing the entire system without human interaction is achieved by using IOT technology [16]. Every component is already available on the internet, IOT just provides the connectivity between the devices and the embedded system that is much beyond the concept of the machine - to - machine and machine-to-human interaction. It is accessing the data that is collected in a systematic manner and several protocols are followed in specific domains to get hold of the front-end applications that are used by users. The main components of IOT technology are:

- Hardware: all the physical devices, sensors, actuators, and communication systems that are embedded in one place.
- Middleware: the mechanism used for storing the data that is collected and analyzing the data with specific tools [4].
- Presentation: the accessing part where visually the uploaded data is available and is accessed by the concerned user anytime needed [17].

A. Chronology of IOT:

The use of IOT was dated back in the 1980s. When the members of Carnegie Mellon Computer Sci. Dept. thought of bringing minor alterations in the current bending machine of the institute. They simply added micro-switches to their present Coke vending machine and through a hardwired network connected the output port with the PDP-10 departmental computer [16]. The only information that was observed on the output side was: number of total bottles in the machine, whether the bottles are cold or hot. This was the basic concept from where IOT was born. After that, for almost two decades no major reforms were brought in this technology.

B. The architecture of IOT:

IOT technology is introduced in almost every organization that is doing digital Reformation of their current system. The implementation of IOT technology basically depends on the architecture in which it was introduced. There are two types of architecture involved while installing IOT:

- 3-layer architecture
- 5-layer architecture

3-Layer architecture:

3-layer architecture involves three phases-

- Perception layer: this is referred to as the physical layer that is responsible to collect all sorts of data and information from the user end. In this layer, the things from the physical world are assigned different names as per the digital world. After collecting data, it is stored in the given memory space and used for further activities from there. Whenever a specific need arises to gain access to a specific set of information, it is addressed in this section [18].
- Network layer: This is the interfacing layer between the perception layer and application layer. It is responsible for the assignment of IP addresses to each object or device connected with the system [19]. The processing, broadcasting and accessing of data are done in this layer which is connected to all the devices that are upgraded with IOT technology. Figure 3: Shows the 3-layer architecture.

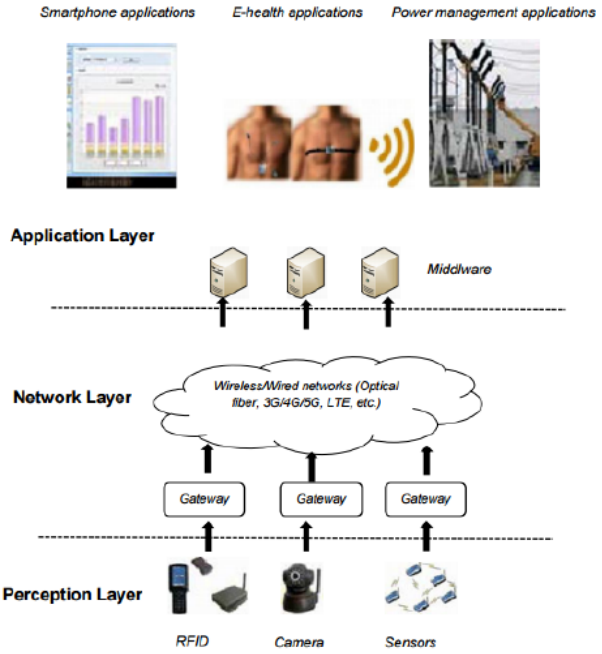

Figure 3: 3-layer architecture [27]

- Application layer: It's the layer where the implementation of the technology happens. The runtime working of all the sensors and actuators involved in interfacing with IOT is seen in this layer [20].

This architecture was used in primitive stages with old generation devices. With the configuration of today's objects, a new architecture is introduced that will give a definitive answer to the present organization.

5-layer architecture:

The 5-layer architecture is made up of five layers that are interconnected with each other.

- Perception layer: It works in the same manner as it does in 3-layer architecture. This is referred to as the physical layer that is responsible to collect all sorts of data and information from the user end. In this layer, the things from the physical world are assigned different names as per the digital world [21]. After collecting data, it is stored in the given memory space and used for further activities from there. Whenever a specific need arises to gain access to a specific set of information, it is addressed in this section, Figure 4: Shows the 5-layer architecture.

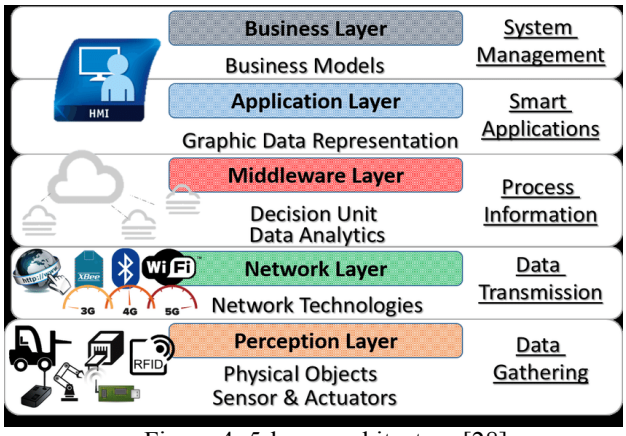

Figure 4: 5-layer architecture [28]

- Transmission layer: As the name suggests, this layer happens to be a path link between the perception layer and the processing layer. The data accumulated in the first layer is taken to the next steps via any networking technology available. One can use LAN, 3G, 4G, LTE, RFID, etc. to create a gateway for data transmission between two layers [22-29].
- Processing layer: It is the core of implementing IOT. The most crucial role in processing the information/data collected from the first layer is done by processing laid. With the help of cloud computing, data is assigned specific places from where they are accessed during runtime. When the user requires any of the predefined data that is stored in the cloud, in this layer it is fetched and used further [30].
- Application layer: This works in the same way as it does for three-layer architecture. It's the layer where the implementation of the technology happens. The runtime working of all the sensors and actuators involved in interfacing with IOT is seen in this layer [31].
- Business layer: It is the last layer that is responsible to manage the working structure of IOT. All privacy-related problems are defined here and taken care of in the runtime application of IOT [20].

IV. Methodology

To study IOT and perform research analysis on it, a Quantitative method is used. A census is prepared on the people resorting towards IOT technology and statistical analysis is done on the problem statement. Graphs and charts are prepared based on smart devices used by the people of concern. Only statistical analysis and graphs regarding the topic are obtained under this methodology.

Data sampling and analysis: it is done by collecting data from a random group of 250 people from a specific area through IOT devices. It's checked on the recipient's end about whether the message received was the same as the original or the distorted one. Samples taken are totally decided by the organization in the concerned area.

Questionnaire method: the main objective is to reach every individual and analyze their viewpoints on the system. The best way to reach thousands of people is to reach by means of a survey. A questionnaire is prepared and 250 people in the concerned department are asked to fill up. It involves open index and close index questions. Here they can mention the devices they are using, problems they are facing, so far experience with the technology, and give suggestions from their end. The responses given by them are classified into two categories: negative and positive. A final report is made based on the responses sent by them and each question is evaluated in general. After the evaluation, the company is notified of the expected changes that the employees are demanding and let them know about the present scenario.
A group of 250 employees was targeted for working in the IT department of the organization. Company X was dealing with consumer products and has recently upgraded its billing system to IOT technology. These employees were the first group to be addressed with IOT. After a month of training and experience of using the technology, a survey was taken to understand how they have coped up with new technological reforms. A list of questions was prepared that was divided into two categories: open index questions to know about their experiences and their suggestions and close index questions that were full of numbers and statistical analysis.

V. Results:

The number of individuals taken into account were 250. A survey taken for their satisfaction level shows that 22% were highly satisfied and 22% were highly dissatisfied from the deployment of IOT in the present system. 30% remained neutral and were found to be actively supportive along the process and were willfully dedicated to understanding the system changes, Figure 5 Shows the number of Participants.

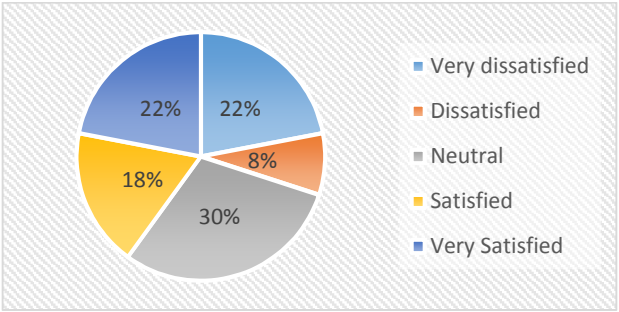

Figure 5: Participants (Created by author)

The results show that when IOT was deployed in the existing software, the effectiveness level between the participants variegated drastically. Level 1 was considered to be most ineffective and level 5 was considered to be highly effective showing, 33% of the sample space taken responded well after the deployment of IOT and 7% were finding it very difficult to cope up with the system due to lack of knowledge and unwillingness to accept the change, Figure 6: Shows the Effectiveness level.

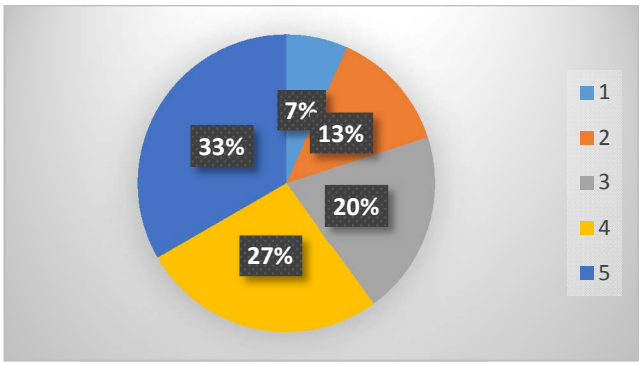

Figure 6: Effectiveness level (Created by author)

VI. Conclusion

The research work on collecting data and storing it using cloud assisted IOT technology is done in a minutely approached manner. The research questions imposed in the early phase of the project were answered with suitable explanations and diagrammatic representation. A questionnaire methodology was taken to do an analysis of the complete system. By the results obtained, it was clear that with the world going digital, IOT technology is the best interfacing technology that can work precisely and accurately for the given organization and give fruitful results. The data that is accumulated is stored and accessed with full security measures and leakage is prevented to the maximum extent.

References

[1] R. Kitchin, The data revolution: Big data, open data, data infrastructures, and their consequences., 1st ed. Sage Publications Inc, 2014.

[2] H. Lin and N. Bergmann, "IOT Privacy and Security Challenges for Smart Home Environments", Information, vol. 7, no. 3, p. 44, 2016. Available: 10.3390/info7030044.

[3] Y. Ghamri-Doudane, R. Minerva, J. Lee and Y. Jang, "Guest Editorial Special Issue on World Forum on Internet-of-Things Conference 2014", IEEE Internet of Things Journal, vol. 2, no. 3, pp. 187-189, 2015. Available: 10.1109/jIOT.2015.2428951.

[4] N. Gupta, "Internet of Things (IOT): A Vision of Any-Time Any-Place for Any-One", International Robotics & Automation Journal, vol. 2, no. 6, 2017. Available: 10.15406/iratj.2017.02.00041.

[5] S. Zanjal and G. Talmale, "Medicine Reminder and Monitoring System for Secure Health Using IOT", Procedia Computer Science, vol. 78, pp. 471-476, 2016. Available: 10.1016/j.procs.2016.02.090.

[6] J. Moorthy et al., "Big Data: Prospects and Challenges", Vikalpa: The Journal for Decision Makers, vol. 40, no. 1, pp. 74-96, 2015. Available: 10.1177/0256090915575450.

[7] C. Yang, "Geospatial cloud computing and big data", Computers, Environment and Urban Systems, vol. 61, p. 119, 2017. Available: 10.1016/j.compenvurbsys.2016.05.001.

[8] D. Tiwari and G. Gangadharan, "SecCloudSharing: Secure data sharing in public cloud using ciphertext-policy attribute-based proxy re-encryption with revocation", International Journal of Communication Systems, vol. 31, no. 5, p. e3494, 2017. Available: 10.1002/dac.3494.

[9] H. Saha, A. Mandal and A. Sinha, "Recent trends in the Internet of Things", 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), 2017. Available: 10.1109/ccwc.2017.7868439 [Accessed 6 September 2019].

[10] N. Vaghela, "RFID and IP Based Object Identification in Ubiquitous Networking", International Journal of Distributed and Parallel systems, vol. 3, no. 5, pp. 139-147, 2012. Available: 10.5121/ijdps.2012.3512.

[11] A. Vijayaraghavan, "Implementation of Secured IPv6 for 6LoWPAN Based Internet of Things", International Journal of Computing and Business Research, vol. 7, no. 1, p. 9, 2017. Available: 10.26519/ijcbr.2017.7.1.02.

[12] K. Sharma, "Safety in Wireless Sensor Network: Types of Attacks and Solutions", International Journal Of Engineering And Computer Science, 2016. Available: 10.18535/ijecs/v5i12.35.

[13] M. Banâtre, Cooperating embedded systems and wireless sensor networks. Hoboken, NJ: Wiley, 2008.

[14] S. Gerlinger, "A wired connection: Parental engagement and digital technologies", Mount Royal Undergraduate Education Review, vol. 1, no. 1, 2014. Available: 10.29173/mruer120.

[15] S. E.W., A. S.J. and B. D.L., Global RFID: the value of the EPCglobal network for supply chain management. Springer Science & Business Media.. 2007.

[16] S. W.D., The Future is Smart: How Your Company Can Capitalize on the Internet of Things--and Win in a Connected Economy., 1st ed. 2018.

[17] T. Hui, R. Sherratt and D. Sánchez, "Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies", Future Generation Computer Systems, vol. 76, pp. 358-369, 2017. Available: 10.1016/j.future.2016.10.026.

[18] Y. Li, X. Cheng, Y. Cao, D. Wang and L. Yang, "Smart Choice for the Smart Grid: Narrowband Internet of Things (NB-IOT)", IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1505-1515, 2018. Available: 10.1109/jIOT.2017.2781251.

[19] A. Ghasempour, "Internet of Things in Smart Grid: Architecture, Applications, Services, Key Technologies, and Challenges", Inventions, vol. 4, no. 1, p. 22, 2019. Available: 10.3390/inventions4010022.

[20] M. Pandith, "Data Security and Privacy Concerns in Cloud Computing", Internet of Things and Cloud Computing, vol. 2, no. 2, p. 6, 2014. Available: 10.11648/j.IOTcc.20140202.11.

[21] IOTWorm, "Internet of Things Connectivity Challenges - IOT Device Connectivity", IOT Worm, 2015. [Online]. Available: https://IOTworm.com/internet-of-things-connectivity-challenges/. [Accessed: 20- Sep- 2019].

[22] S. Malwa, "Wireless 2.0 — Integrated Networks on the Blockchain.", Hackernoon.com, 2018. [Online]. Available: https://hackernoon.com/wireless-2-0-integrated-networks-on-the-blockchain-caa09a61913b. [Accessed: 21- Sep- 2019].

[23] V. Thayananthan, O. Abdulkader, K. Jambi and A. Bamahdi, "Analysis of Cybersecurity Based on Li-Fi in Green Data Storage Environments", 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 2017. Available: 10.1109/cscloud.2017.32 [Accessed 21 September 2019].

[24] W. Suparta, "Application of Near Field Communication Technology for Mobile Airline Ticketing", Journal of Computer Science, vol. 8, no. 8, pp. 1235-1243, 2012. Available: 10.3844/jcssp.2012.1235.1243.

[25] K. Yayla and S. Burmaoğlu, "USING RFID (RADIO FREQUENCY IDENTIFICATION) TECHNOLOGIES ON HOSPITALS: A LITERATURE REVIEW", 2015. [Accessed 21 September 2019].

[26] S. Shao et al., "An Indoor Hybrid WiFi-VLC Internet Access System", 2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems, 2014. Available: 10.1109/mass.2014.76 [Accessed 21 September 2019].

[27] M. Abdmeziem, D. Tandjaoui and I. Romdhani, "Architecting the Internet of Things: State of the Art", Robots and Sensor Clouds, pp. 55-75, 2015. Available: 10.1007/978-3-319-22168-7_3 [Accessed 21 September 2019].

[28] L. Antao, R. Pinto, J. Reis and G. Goncalves, "Requirements for Testing and Validating the Industrial Internet of Things", 2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), 2018. Available: 10.1109/icstw.2018.00036 [Accessed 21 September 2019].

[29] A. S. Shibghatullah and I. Al Barazanchi, "An analysis of the requirements for efficient protocols in WBAN," J. Telecommun. Electron. Comput. Eng., vol. 6, no. 2, 2014.

[30] H. R. Abdulshaheed, S. A. Binti, and I. I. Sadiq, "Proposed a Smart Solutions Based-on Cloud Computing and Wireless Sensing," Int. J. Pure Appl. Math., vol. 119, no. 18, pp. 427–449, 2018.

[31] I. Al Barazanchi, H. R. Abdulshaheed, S. A. Shawkat, and S. R. Binti, "Identification key scheme to enhance network performance in wireless body area network," Period. Eng. Nat. Sci., vol. 7, no. 2, pp. 895–906, 2019.