1-2022

Relevance of Internet of Things to Health Institutions in Clinical Data Management: Implication for Librarians

Faith O. Mesagan
University of Nigeria, Nsukka, faith.mesagan@unn.edu.ng

Moses Elechi
Cross River University of Technology

Francis O. Adurota
University of Nigeria, Nsukka

Chinedu Obinna Ejimonye
Alex-Ekwueme Federal University Ndufu-Alike Library

Onyinyechi G. Ossai
University of Nigeria, Nsukka

Relevance of Internet of Things to Health Institutions in Clinical Data Management: Implication for Librarians

Faith O. Mesagan[1], Moses Elechi[2], Francis O. Adurota[3], Chinedu Obinna Ejimonye[4]
Onyinyechi G. Ossai[5]

[1]Department of Library and Information Science, University of Nigeria, Nsukka

[2]Department of Electrical Electronic Engineering, Cross River University of Technology, Calabar

[3]Center for Lion Gadgets and Technologies, University of Nigeria, Nsukka

[4]Reader's Services Department, Alex-Ekwueme Federal University Ndufu-Alike Library, Ebonyi State, Nigeria

[5]Department of Geography, University of Nigeria, Nsukka

Corresponding author: Francis O. Adurota, Center for Lion Gadgets and Technologies, University of Nigeria, Nsukka (email: olalekan.francis@unn.edu.ng)

Abstract

The Internet of Things (IoT) is the internetworking of physical devices which consists of an embedded system with sensors, actuators and network connectivity that enable collection and exchange of data. Each day, we are witnessing the emergence of new technologies that have the capability to embed into our environment and measure the physical, social and contextual phenomenon. The technology behind IOT is driven by various technological forces such as smart devices, wireless network, and pervasive connectivity among others. Data collection, management and accessibility are made easy with Internet of Things IOT. The Internet of Things (IoT) is aimed at formulating a complex information system with the combination of sensor data acquisition, efficient data exchange through networking, machine learning, artificial intelligence, big data, and clouds. This paper, therefore, focused on the relevance of Internet of Things (IoT) in clinical data management for health institutions. This includes the impact on how data are collected, how they were being analyzed and stored, and its impact in terms of security and privacy-related issues.

Keywords: Big Data, Clinical Data, Internet of Things, Librarians, Privacy, Security

INTRODUCTION

Internet of Things (IoT) technology, are today part of our lives and most evident in every major facet of our lives of which health institutions are not left out. In hospital emergency wards, the severity of tasks posed serious health risks to patients. Patient management when achieved through conventional methods generally result in management breakdowns. Hence, there is a degradation in the performance of efficient management approaches. Many healthcare institutions in Nigeria suffer from a plethora of inefficiencies and dysfunctions. Though the Government and individuals are putting much effort into (new hospitals, rehabilitations of old ones, training of new physicians among other things), but the problem still persists and medical staff, patients and globally health system are severely affected. Because of the aforementioned, this study is carried out to consider the impact of IOT to health institutions in clinical data management, and as such variables that are principally linked to mismanagement of health related activities, equipment, human and material resources will be reveal. Sabooniha, Toohey and Lee (2012) in their study determined the influence of human resource management on the improvement of healthcare delivery in public hospitals and discovered that good management leads to a better healthcare delivery quality. Other similar studies include that of Pocztowski (2010). Jończyk (2015) was of the opinion that it is necessary to note that the artifacts used during work are essentially limited to Excel paper sheets, which are often not updated and sometimes even get lost between the different services. This problem exists as a result of the excessive yet crucial work volume imposed on the personnel, which decreases the efficiency of work and healthcare delivery quality. Inasmuch the lofty aim of every healthcare organizations is to provide cost effective, high quality, shared and seamless healthcare delivery, they need to reduce medical errors, safeguard patients' data and streamline clinical and administrative tasks is very much important. The numerous studies that have been carried on this issue have almost shown the importance of management and management breakdowns among the

medical staff members that inevitably have an impact on the quality of care provided to patients and put them in a potentially vulnerable and dangerous situation (Sabooniha, Toohey & Lee, 2012).

In this paper, there is need to consider the Governance, Risk and Compliance approach (GRC) coupled with Internet of Things technology (IoT) called tGRC. This study is done to help provide a set of tools that may effectively address core medical needs and improve the quality of patients' care. One can propose an effective support enabling management features of the related tasks as well as providing an efficient data collection in real time awareness around the occurring events; particularly those which constitute a priority in any health institution. We led a study in a Nigerian maternity ward to comprehend the methodology in which medical activities are achieved by medical staff like midwives, gynecologists-obstetricians, nurses, anesthetists etc. and to identify the principal artifacts in management and coordination. If for instance, one can begin by analyzing the way with which medical staff collect information, operate with different medical scenarios, and how they manage the work. It might be evident that the medical staffs are suffering under the load of all the procedural, intellectual and social complexity of the management process. Indeed, the heavily accumulated volume of data ought to be collected, processed and made available for appropriate use.

Literature Review

According to Ovidiu and Peter (2013), it can be referred to the general idea of things, mostly everyday objects, which can be readable, recognizable, locatable and addressable through information sensing device and control through the Internet, regardless of the means of communication. Internet of Things (IoT) is an extension of the Internet where large numbers of "things", such as sensors, actuators and processors, including human users, are networked and able to provide high resolution data on their environment and exercise a

degree of control over it (Peter & Richard, 2017). Internet of things does not only include electronic devices as we see on daily basis such as vehicles and equipment but also include food, water, clothing, people, phones, chairs among others interacting with one another. Internet of things according to Keyur and Sunil (2016) is an internet of three things which include: people to people, people to machine /things, and things /machine to things/machine, interacting through internet. Laith, Rupak, Omprakash, Marcela, and Ali (2018) observe that IoT is a symbiosis of various technologies and is going to change drastically what can be achieved from the internet currently.

DOMAIN MODEL FOR HEALTH INSTITUTION APPLICATION BASED ON IOT

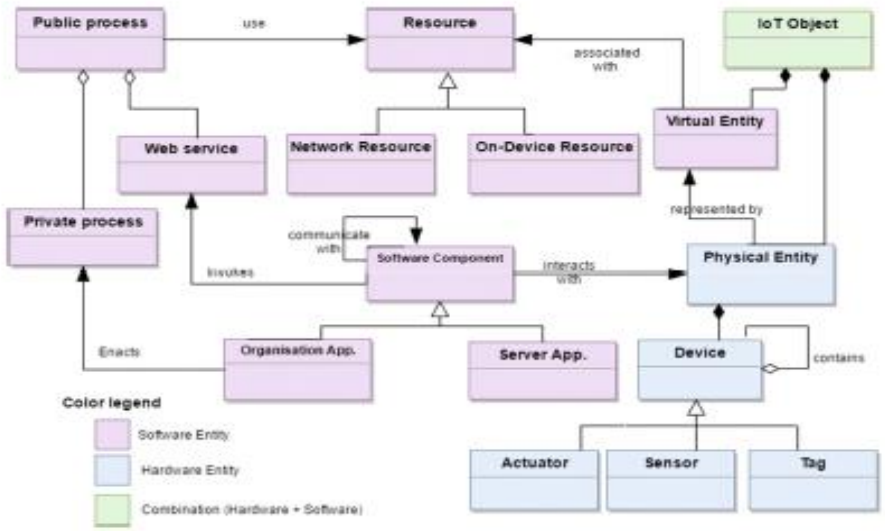

Fig. 1. Domain model of health institution application based on IoT

The above diagram is a conceptual model for a health institution applications based on IoT. The model is founded on advanced enterprise systems (Benmerzoug, 2015) and those of the IoT domain (Haller, Serbanati, Bauer & Carrez, 2013). As seen, it is composed of domain entities and shows the interrelating pathways that can exist between those entities. A public process is the aggregation of the private processes and/or Web services participating in it. It can be noted here that private processes are considered as the set of processes of the organization itself and they are managed in an autonomous way to serve local needs. The

public processes span organizational boundaries. They belong to the organizations involved in a collaboration relationship and have to be agreed and jointly managed by the different partners. The most generic IoT scenario is seen as a generic Agent (human or software component) needing to interact with a physical entity in our tangible world. Physical entities are represented in the digital world by a virtual entity. An IoT object (or a thing) is the composition of a virtual entity and the physical entity it is associated to, in order to highlight the fact that these two concepts belong together. One should realize that the device entity will often perform in a bi-directional manner with the "IoT object" at the edge of the network either acting as input devices (sensors) or output devices (actuators). Besides input and output devices, tags are used to identify physical entities, to which the tags are usually physically attached. The identification process is called "reading", and it is carried out by specific sensor devices, which are usually called readers. The primary purpose of tags is to facilitate and increase the accuracy of the identification process. Public process (which is the aggregation of the private processes and/or web services participating in it) consumes resources. Resources are software components used in the actuation on physical entities. There is a distinction between on-device resources and network resources. As the name indicates, on-device resources are hosted on devices (like software that is deployed locally on the device). They include executable code for accessing, processing, and storing sensor information, as well as code for controlling actuators. On the other hand, network resources are resources available wherein the network, e.g., back-end or cloud-based databases. A virtual entity can also be associated with resources that enable interaction with the physical entity that the virtual entity represents.

Clinical Data Management

It is quite obvious that the amount of data generated in a hospital is voluminous as this information though sometimes proving innecessar is still much valued in forecasting, drawing

a correlation and regression as well as real time monitoring. For example, if one is to look at the real time information of the blood pressure and temperature readings of a near comatose patient, its much evident one would tire from all the cumbersome data. Hence in order to effectively and efficiently use this information all processes will require rigorous execution for a better result, the following becomes imperative.

Quality Assurance (QA) in this processes are ensuring that the clinical data presented and interpreted in the clinical study report reflect a true picture of what took place in the trial. While according to ICH GCP definition QA include all those planned and systematic actions that are established to ensure that the trial is performed and the 'clinical' data are generated, documented (recorded), and reported in compliance with GCP and the applicable regulatory requirement(s) (Benmerzoug, 2015). It is necessary that clinical data management have written procedures in place which will allow an independent group to audit against the actual processes taking place in the handling of clinical data. The documentation detailing what has happened during that operation should be present. The presence of a QA group is perceived as of marginal importance, certainly in the view of senior management. However, there is no doubt that the inclusion of quality in the culture of a company or organisation is a requirement of any operation conducting clinical operations. The last principle of ICH GCP requires that there are 'systems with procedures that assure the quality of every aspect of the trial' (Rondel, Varley & Webb, 2020).

Quality Control (QC) based on The definition in the ICH GCP definitional guidelines for QC is the operational techniques and activities undertaken within the quality assurance system to verify the requirements for quality of the trial-related activities have been fulfilled (Benmerzoug, 2015). It explains the necessity of clinical data management having documented evidence of what so ever activity has been carried out through any clinical operation ensuring the quality of the clinical data. QC tasks are the responsibility of the

personnel handling the clinical data. In some cases, most often group designated within clinical data management to conduct these tasks.

Audit is a systematic and independent examination of trial related activities and documents to determine whether the evaluated trial related activities were conducted, and the 'clinical' data were recorded, analysed and accurately reported according to the protocol, sponsor's standard operating procedures (SOPs), GCP, and the applicable regulatory requirement(s) (Benmerzoug, 2015). A necessary audit plan is much needed and the main scope should be recorded in the resulting audit report. Normally, key questions will have been listed before the audit has commenced and the auditor should be encouraged to restrict his/her attention to the audit's scope.

Performance defines a measure of fitness for purpose and can be used as an overall measure of quality and productivity or work rate. We will be looking at three primary performance indicators, *productivity, quality* and *process cycle times*. In performance, a *standardized* set of process tasks must be clearly defined. The data management process flow is changing and developing quickly as new technology is introduced to the data collection process. It is difficult to consistently define the process flow as there is often much variation across organisations, clinical phases and therapeutic areas. However, in order to define comprehensive performance standards, it is critical our measurement tools on a common set of processes within data management which can be consistently interpreted across clinical phases, therapeutic areas and indeed organizations. It is therefore important to define the work flow process in clinical data management using IOT.

DEFINING THE PROCESS FLOW

A summary of key data management tasks is presented below and will be used as a focus for performance measurement:

- *Data collection*: Data can arrive in an electronic format, such as laboratory data from central laboratories, diary card data collected on hand-held computers or via interactive voice response systems, or more directly via remote data entry systems and remote data capture solutions.
- *Pre-entry data review* (secondary monitoring). Often, a pre-entry manual review of all source CRF data is made to ensure completeness of data. Some data may be coded at this stage to support the data entry process. Data queries may also be raised at this stage.
- *Data entry.* Following receipt of data from the investigator site, data are keyed or loaded onto the clinical database. Most data entry teams enter CRF data via an independent double data entry process with either a file extract and compare process or via an on-line verification process to ensure data quality at this key stage in the development of the database
- *Data validation.* Data are cleaned in a batch process using validation programmes which have been specified and developed before data entry commences. The majority of data queries are generated at this stage.
- *Term coding.* Adverse event data, concurrent medications and medical conditions are often coded using standard dictionaries both using an auto encoder and via manual coding. Again, this is often a batch process.
- *Database editing.* The developing database is edited following batch receipt of resolved data queries from the field.

Process tasks listed above are by no means comprehensive but typically summarize the in-process flow for data management

The Proposed Information System Architecture Based on IOT Technologies

As confirmed by a survey in several Swiss hospitals at 2009 (Rondel, Varley & Webb, 2020), 64% of them replied that the healthcare sector is a complex and heterogeneous economic sector and cannot be compared to other industry sectors where Control Objectives for Information and related Technology (CobiT) and other IT governance framework have been successfully applied; hence, the use of this particular information structure. Here, specific sensors are used to collect comprehensive physiological information and uses gateways to send data to the server on the Cloud for analysing and storage. Information is sent after to medical-staff wirelessly. Our proposition is shown in the figure below

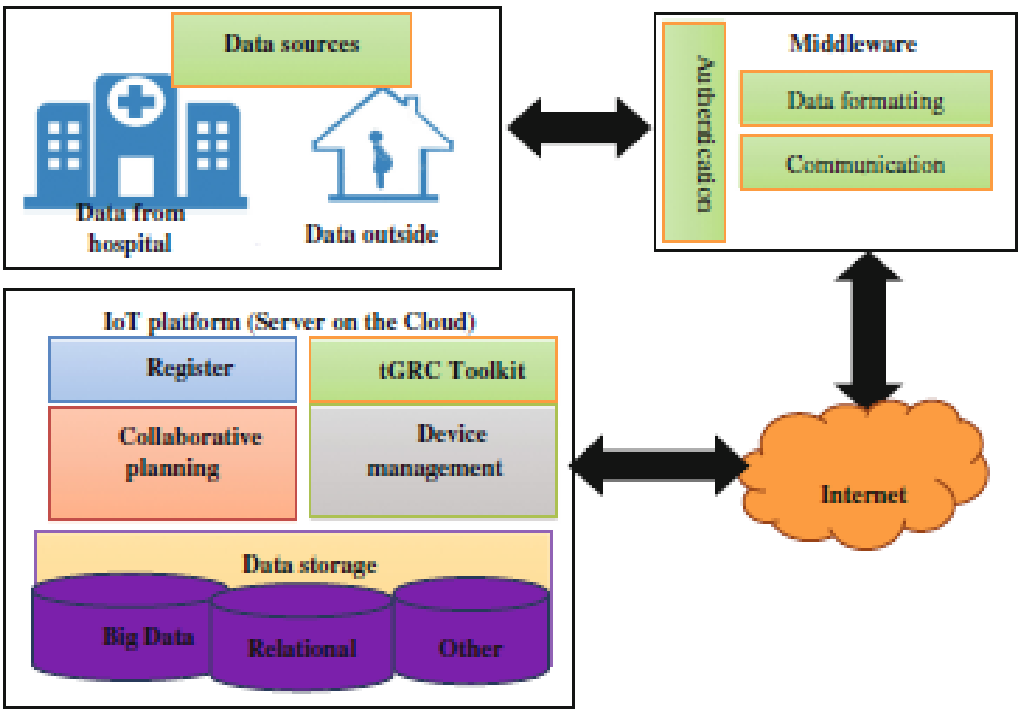

Fig 2 A Proposed Structure

For data collection the use of the IoT solutions greatly improves the quality of care through continuous attention and lowers the cost of care by eliminating the need for a medical-staff to actively engage in data collection. In addition, the technology can be used for remote monitoring using small, wireless solutions connected to patients through the IoT

capabilities. Data is collected from different sources: Wearable devices or from sensors (installed on different equipment).

- The Middleware plays the role of a gateway, it intercepts data sent by the various sensors to the software platform located in the cloud to be stored and analysed. The middleware performs an authentication operation to identify the device; it formats data under to specific shape before sending it to the server. The formatting operation facilitates the server work, it minimises the time of data recognition operation.
- The IoT Platform Components: In what follows the most important constituents of the server on the Cloud architecture are highlighted. First, the register contains a list of IoT devices and different equipment that collect data, it used to control and to avoid any external and unwanted attempts to connect to the server or to the gateway.
- The Device Management module: is used to manage objects connects to the IoT platform. User can add, remove and configure devices remotely.
- Collaborative planning module: this module allows an efficient planning with a collaborative manner. Hence health care task planning process is fundamentally a collaborative task that requires the participation of many health care experts with different skills working simultaneously on same cases. It's based on a collaborative planning approach and it constitutes an evolution of planning environments toward new shared workspaces supporting collaboration.
- The Data Storage module takes care of the collected data storage either inside or outside the hospital. It uses relational databases as well as big data techniques or any data storage technology. This section provides the user a fast, secure and efficient access to all patient, medical and other resources information.

- The tGRC module enables the health institution to manage risk and regulatory issues across the organization. It provides a set of essential services and functional components that encompass various areas of risk and compliance management.
- The tGRC solution legal register offers access to the legal universe for each act. Fully searchable, tGRC solution gives the needed law easily and rapidly. The stakeholders can give feedback on the published information. This feedback is sent to the rules database. Finally, the rules administrator can improve and communicate about this information.

Accordingly, the proposed modelling step aims at a balanced consideration of both compliance and risk factors while incorporating the risk attitude of governance maker regarding the IoT systems specificity and the Cloud offers.

The model aims to set goals to reach global objectives. Formally objectives are:

$$tObjectives = \left\{ \text{Ethical}_{\text{cor-decision}}, \text{Efficiency}_{\text{improv}}, \text{Effectiveness}_{\text{improv}} \right\}$$

These three objectives for IoT systems based on tGRC concepts form a solid basis for evaluating the IoT systems and Cloud offers solution which could be extended in practice by more detailed and specific objectives. For example, the security objectives have to be detailed by authentication, authorization, accounting, etc. The model developed here is meant to act as a risk minimization and compliance maximization tool, that is, it is supposed to identify the Cloud Computing service or the combination of services which causes the optimal cost for an organization by taking risk and compliance issues into account.

Reasons or objectives of introducing IOT in clinical data management cannot be over emphasized which include: to obtain valid patient data via Case Record Forms (CRFs) as required by the protocol; ensure immediate availability of data in the company (the time gap

from site to database should be minimal); ensure immediate processing of incoming data (including plausibility/validity checking/database finalization); provide validated databases, both the initial application and upgrades, for product registration and other company needs; enable compilation of global and project databases composed from local databases (international clinical trial) for statistical reporting and tabulations; provide necessary access to the data of an ongoing trial to satisfy drug safety aspects, ethical and legal requirements; fulfill GCP requirements with respect to clinical data processing. Just as the objectives are all encompassing, so also are the objectives and these makes IOT a necessity in health institutions.

Importance of IOT in health management

From all indications, it will not be out of place to state here that the importance of IoT is to connect smart objects (referring to things) to the Internet in a transparent way thereby leading to an exchange of data between all things, and bring health users information in a more secure way. According to Riazul, Daehan, and kwak, cited in Gonçalo and Vitor (2019*)* healthcare is one of the most attractive applications fields for IoT making available the possibility of many medical applications such as remote health monitoring, fitness programs, chronic diseases, and elderly care. As we all know, healthcare is an important priority for all (governments inclusive) as it relates to population growth, rural urbanization, declining birthrate, population aging, economic growth and social unbalanced resource utilization. Some social problems have become increasingly apparent in the healthcare field; some of these issues in healthcare that IoT can combat in a most effective way (Gonçalo & Vitor, 2019) includes*:*

- health management level and the incapability of responding to emergency;

- serious shortage in medical staffs and institutional facilities especially in rural areas, lack of medical facilities, low level of treatment, inadequate healthcare system;
- Imperfect diseases prevention system cannot meet the national strategy requirements to safeguard the health of the citizen resulting in an heavy burden on economy, individuals, families and State;
- Inadequate disease prevention and early detection capability
- There are technologies that are useful in healthcare environment which can be adopted in IOT-based healthcare system to the benefit of both patients and provider stand to benefit from.
- Reduction in cycle time from protocol development to report
- Improved Regulatory Compliance (complete audit trails, CANDAs)
- Improved data integrity and quality, tracking techniques
- Improved efficiency and utilization of resources
- Facilitated clinical research monitoring capabilities
- Improved project management and planning capabilities
- Reduction or maintenance of project costs.

Challenges associated with the use of IOT such as cyber security, lack of basic infrastructure

One of the major challenges in Nigeria over the years is the issue of security which networks is not excluded. Therefore, security, privacy and trust are critical factors for IoT applications as well. Laith et al. (2018) were of the opinion that when packets are routed through different links and devices to reach ultimate receiver on the internet, measures should be taken so that the confidentiality and integrity of the data is maintained. It was clearly stated that:

> IoT devices are low power constrained devices, therefore, already established cryptographic solutions cannot be directly applied in the IoT scene. More so, the integration of application in the network infrastructure is focused on only achieving the functionality rather than holistically considering the security requirements when the application is designed (Laith et al. 2018, p.5).

There were warning from cybersecurity experts on IoT as the most vulnerable technology as they expect more targeted attacks on existing and emerging infrastructures such as data theft, physical injury, ransomware for smart homes or smart cars among others. Other challenges include:

Trust and data integrity which enables one to ensure the data sent has not changed from the moment it is sensed until it reaches the final destination. This involves verifying the data and validating the verification certificate. Trillion points of vulnerability is a situation where each device connected to IoT represents a potential risk and leads to questions - how confident can an organization be of the data gathered and the integrity of the data sent? How to make sure data has not been interfered or compromised with? These and many more were the issues arising from IOT vulnerability.

Data protection*:* considering a country like ours where copyright protection has not been properly implemented in an online environment one begins to be more curious if there will be require law to be designed to protect and control individual and organization data gathered by sensors or applications and stored to be part of a filing system.

Data privacy*:* is to protect the data from exposure in the IoT environment. For instance, any logical or physical entity can be given a unique address and the ability to communicate automatically over the network.

Challenges associated with the use of IoT

As mentioned earlier, one major challenge in Nigeria over the years is the issue of security which networks is not excluded. Therefore, security, privacy and trust are critical factors for IoT applications as well. IoT devices are low power constrained devices;

therefore, already established cryptographic solutions cannot be directly applied in the IoT scene. There were warning from cybersecurity experts on IoT as the most vulnerable technology as they expect more targeted attacks on existing and emerging infrastructures such as data theft, physical injury, ransom-ware for smart homes or smart cars among others. Data Privacy is to protect data from exposure in the IoT environment. For instance, any logical or physical entity can be given a unique address and the ability to communicate automatically over the network.

CONCLUSION

Clinical data managed over IoT platforms are easily accessible over the internet and can be collected from different clinical institutes. The biggest challenge from the regulatory perspective would be the standardization of data management process across institutes, and development of regulations to define the procedures to be followed and the data standards. From security perspective, the biggest hurdle would be the planning and implementation of highly secured infrastructure that will protect the clinical data from hackers.

REFERENCES

Bauer, M., et al. (2013). IoT reference model. In: Bassi, A., et al. (eds.) Enabling Things to Talk, pp. 113–162. Springer, Heidelberg. doi:10.1007/978-3-642-40403-0_7

Bedhief, I. Kassar, M., & Aguili, T. "SDN-based architecture challenging the IoT heterogeneity," in *Proc. IEEE 3rd Smart Cloud Networks Systems (SCNS), Dubai*, Dec 2016.

Benmerzoug, D. (2015). Towards AiP as a service: an agent based approach for outsourcing business processes to cloud computing services. Int. J. Inf. Sys. Serv. Sect. 7(2), 1–17.

Clinical Data Management (2010). Second Edition. Edited by R.K. Rondel, S.A. Varley and C.F. Webb. John Wiley & Sons, Ltd

Gonçalo J. F. C. and Vitor N. (2019). An Overview of IoT and Healthcare. Retrieved https://www.researchgate.net/publication/330933788

Haller, S., Serbanati, A., Bauer, M., Carrez, F. (2013). A domain model for the Internet of Things. In: GreenCom/iThings/CPScom, pp. 411–417.

Jończyk, J.A. (2015). The impact of human resource management on the innovativeness of public hospitals in Poland. Procedia Soc. Behav. Sci. 213, 1000–1007.

Keyur K. P. & Sunil M. P. (2016). Internet of Things-IOT: Definition, characteristics, architecture, enabling technologies, application and future challenges. *International Journal of Engineering Science and Computing.* Accessed via http://ijesc.org

Laith F., Rupak K., Omprakash K., Marcela Q. C. & Ali A. (2018). A Concise Review on Internet of Things (IoT) - Problems, Challenges and Opportunities. Paper presented at the 11th International Symposium on Communication Systems, Networks, and Digital Signal Processing (CSNDSP).

Ovidiu V. S., & Peter F. (2013). Internet of Things: Converging technologies for smart environments and integrated ecosystems. River publishers' series in communications,

Peter J. R. & Richard B. W. (2017). Research challenges for the internet of things: What role can OR play?

Pocztowski, A. (2013). Adding value from human resource development in international assignment. Argumenta Oeconomica Cracoviensia (09), 9–28.

Sabooniha, N., Toohey, D., Lee, K. (2010). An evaluation of hospital information systems integration approaches. In: Proceedings of the International Conference on Advances in Computing, Communications and Informatics, pp. 498–504.

Tan, C.L., Nasurdin, A.M. (2010). Human resource management practices and organizational innovativeness: an empirical study in Malaysia. J. Appl. Bus. Res. 2, 105–115