

## The Internet of Things (IoT) in Information Agencies

Saiful Farik Mat Yatin, Hamima Madona Hussain, Khairul Naimi Khairul Fitri, Khairunnisa Aman, Nurulhazreen Shahidun Jamil

To Link this Article: <http://dx.doi.org/10.6007/IJARBSS/v8-i9/4605>

DOI: 10.6007/IJARBSS/v8-i9/4605

*Received: 19 August 2018, Revised: 27 September 2018, Accepted: 29 September 2018*

Published Online: 15 October 2018

**In-Text Citation:** (Yatin, Hussain, Fitri, Aman, & Jamil, 2018)

**To Cite this Article:** Yatin, S. F. M., Hussain, H. M., Fitri, K. N. K., Aman, K., & Jamil, N. S. (2018). The Internet of Things (IoT) in Information Agencies. *International Journal of Academic Research in Business and Social Sciences*, 8(9), 464–475.

**Copyright:** © 2018 The Author(s)

Published by Human Resource Management Academic Research Society ([www.hrmars.com](http://www.hrmars.com))

This article is published under the Creative Commons Attribution (CC BY 4.0) license. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this license may be seen at: <http://creativecommons.org/licences/by/4.0/legalcode>

**Vol. 8, No. 9, September 2018, Pg. 464 - 475**

<http://hrmars.com/index.php/pages/detail/IJARBSS>

JOURNAL HOMEPAGE

Full Terms & Conditions of access and use can be found at  
<http://hrmars.com/index.php/pages/detail/publication-ethics>



# INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES



## The Internet of Things (IoT) in Information Agencies

Saiful Farik Mat Yatin, Hamima Madona Hussain, Khairul Naimi  
Khairul Fitri, Khairunnisa Aman, Nurulhazreen Shahidun Jamil

*Faculty of Information Management, Universiti Teknologi MARA, Puncak Perdana Campus,  
UiTM Selangor, Malaysia*

### Abstract

The overall purpose of the paper is to provide an overview of the Internet of Things (IoT) to the information agencies (IA) such as libraries, archives, museums etc. The paper involved literature survey of selected academic and research IA in public and private chartered institutions. It examined that development of IoT has invented smart technologies that are not only fundamental but also very powerful business tools and devices applied in IA notably to the information services. In this paper, the author has summarized tangible IoT technologies which are helpful to IA to understand IoT business and highlighted the pros and challenges of Internet of Things (IoT).

**Keywords:** *Internet of Things (IoT), Information Agencies, Information Management, Information Services*

### INTRODUCTION

There are technologies proposed to improve facilities and providing user friendly system because most IA need to use technology in their daily operations. This is a way towards an intelligent, smart, internet, web based, network, virtual, electronic, digital, online, automated, computerized IA or whatever they may called it. And with the internet technologies that offers various advantage, there are one technology called Internet of Things (IoT).

Internet of Things (IoT) can be defined as the use of intelligent connected devices and systems to leverage data gathered by embedding sensors and actuators in machines and other physical objects. IoT is a network of devices includes physical devices and network connectivity which enable the objects to connect and exchange the data. Therefore, it refers to the use of intelligent connected devices and system to obtain data gathered by embedding sensors, machines and other physical objects.

Nowadays, modern IA offer technologies that can improve services and enable users to access the information easily. With the rapid changes in technology and the use of Internet of Things (IoT), IA also needs to adapt the IoT. It is a system of interrelated computing devices, mechanical and digital machines, objects that are provided with a unique identifier and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. By using it, technologies enable to access the material and services faster and easier. Thus, to promote the

services and technologies provided, IA use chat, email, social media, Instant Message (IM) to send the information to the users. The services offered must be similar to the functions and core business of the IA that is sharing factual information, providing a directory or catalogue information which provides access to space and equipment, access to traditional and online collections, consultations as well as training services.

Moreover, this paper discusses the benefits and potential of the IoT for IA. The implementation of IoT enable users to locate the physical location includes call number and classification of materials. There are also varieties of challenges in implementing IoT. The main challenge to implement IoT is financial problem, security and privacy. For information, IA provides open source to the users to access the internet. The security and privacy issues occur when they use username and password to access the website or other sources. This is because all users' information stored in the computer and other people can access to the computer too.

### THE INTERNET OF THINGS (IoT) TECHNOLOGIES

Based on research and analyst firm Gartner Inc, they describes IoT as the network of physical objects that contain embedded technology that can communicate and sense, or interact, with their internal states or the external environment. The technologies are designed to improve the services and facilities efficiency and making IA as a smart IA. The technologies include cloud computing, magic mirror, pressure pad sensor and wireless sensor network (WSN).

#### *Cloud Computing*

Refers to the delivery of on demand of computer resources. Ethically speaking, cloud computer is everything from application to data centres. On the other hand, cloud computing known as software applications that exist online and available to multiple users via the internet. Cloud learning occurs when the basis of cloud technology function to support the use of software in the cloud by providing the data storage and software that enable users accessed in an online.

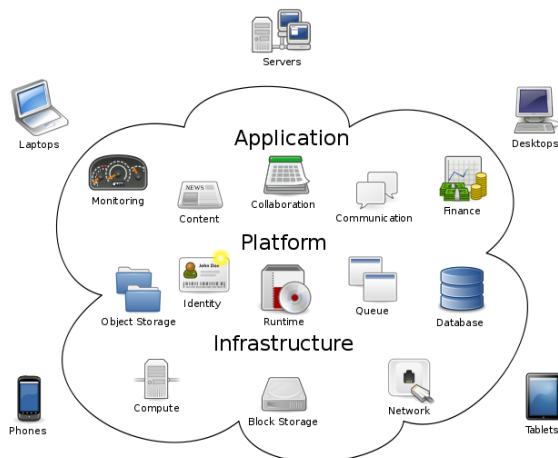


Figure 1: Cloud computing



Figure 2: Magic Mirror

#### *Magic Mirror*

Include cameras and sensors connected to Wi-Fi. It provides interaction between people and computer. Magic mirror contains a lot of data gathering devices data like location recognition,

material recognition in camera and RFID user card detector. Not only that, magic mirror stored information in database. When the user holding any materials, the RFID detects user identity while the camera capturing the information such as title, call number and related information about a material that user browse and carry and pad sensors gather information of where user have been, the specific shelves unit and so forth. Whenever user left the IA with a material in their hand, the system will automatically do the check-out process without the user have need to do it over the counter as traditional practice.

#### *Pressure Pad Sensor*

It consists of a thin sheet sensor pad which enable with Wi-Fi technology. This technology is connected to processing unit which records and control system. Pressure pad sensor is connected to wireless sensor network (WSN) that will detect how many people searches the materials around the shelves. So, from this technology, IA can detect the highest and famous field and materials in the collection and custody.

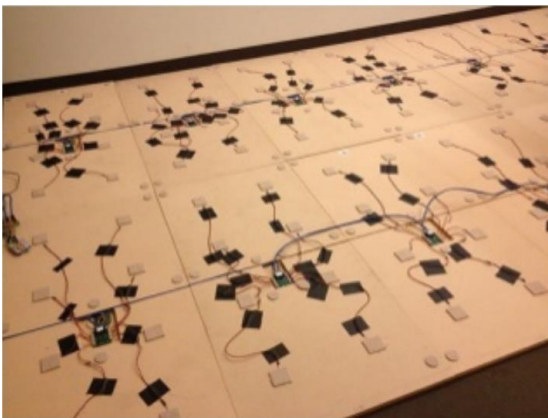


Figure 3: Pressure Pad Sensor

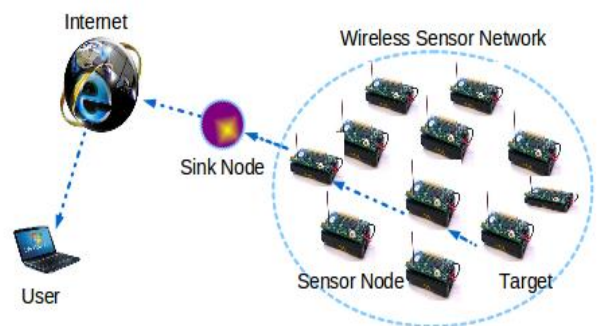


Figure 4: Wireless Sensor Network

#### *Wireless Sensor Network*

It can be defined as the ensemble of spatially distributed, autonomous sensors that cooperate to monitor physical or environmental quantities of interest. The wireless sensor network (WSN) is a network that formed by a large number of sensor nodes where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure and so on. This technology is efficient, low cost, low power miniature devices for use in remote sensing applications.



Figure 5: RFID

*RFID (Radio Frequency Identification)*

There are two components of RFID system which are electronic tags and readers. Electronic tags can be attached to objects to be identified while readers can read or write. It is depending on the memory structure and technology. In IA, when use RFID systems, the reader sends out electromagnetic waves within a region which depends on the operating frequency and antenna size. Then electronic tag has a LC series resonant circuit and its frequency is same with the transmitting frequency of the reader. Nowadays, RFID use in IA for many purposes consists of tagging, check-in/check-out, self-check in/out, shelf management, book drop and anti-theft detection. These purposes ease Information Professional (IP) to accomplish their task faster and helps user to check in/out their books by their self.

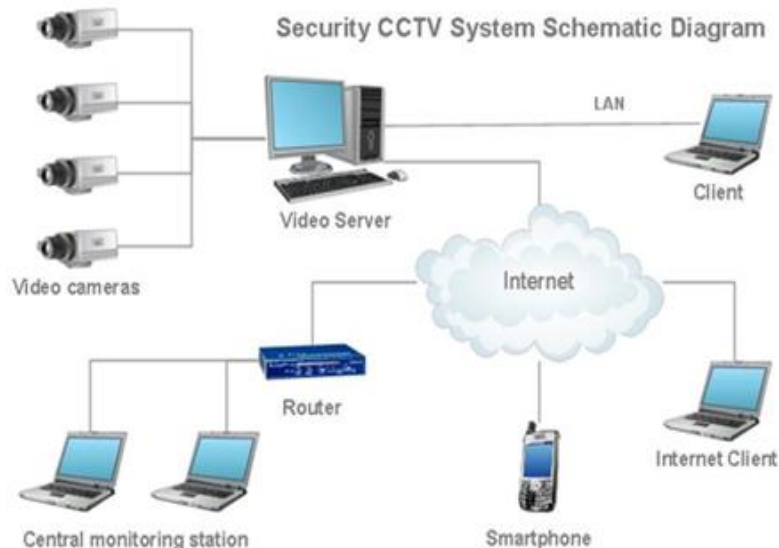


Figure 6: CCTV

### *CCTV (Closed-Circuit Television)*

CCTV can be defined as a TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes. Nowadays, IA use CCTV to monitor the collection and equipment in the IA. For example, CCTV can be used in IA to monitor the user activities and their behaviour in the IA. The common mischievous activities in the IA like tearing of the pages from the books, hiding the books and book theft can be reduced.

### **BENEFIT OF INTERNET OF THINGS (IoT)**

The spread of digital technologies offers a massive potential for the creativity and innovation in all aspects in our daily lives. We are connected to cars, smart homes, connected wearable's, smart cities and connected healthcare. Therefore, IoT become vital technology to help people either at home, work or organizations. Internet providers as well as supplier for example electricity, home and office equipment, gadgets to compete and produce the latest products that meet the needs of users.

IoT *improve services* in IA where checking availability of equipment and providing more detailed, contextual information of collection. The use of IoT to identify areas of IA activities as well the technology performs well. Closed-Circuit Television (CCTV) is a one example of IoT helps Information Professional (IP) to monitor the collections in IA. Therefore, CCTV is generally used for monitoring continually or to monitor one area. CCTV has been proven to be effective either for constant monitoring or for monitoring only an area. Furthermore, CCTV applications do not have limit. By providing CCTV in IA, the collection and other equipment are in safe condition. Thus, IoT helps Information Professional (IP) to identify on detailed the collection and materials.

The use of IoT helps Information Professional (IP) in *streamlining back-office processes*. It helps Information Professional (IP) to accomplish their works in inventory control, organizing access and authentication processes. Moreover, IoT also monitor collection storage in IA.

Besides that, IoT helps user in *education which organizing self-guided tours for user*. The applications IoT in IA can guide the users to identify the location about resources they need. They can search on detail about the material includes the author, title and publication. IoT help users to access the digital materials in IA includes electronic books and electronics journal.

Other benefit is IoT *helps in promotion IA to public*. The use of IoT as a promotion tools and a chance to build a positive image of IA as modern institution. This is a way to attract the users come to IA in order to promote the collection of materials.

IoT *helps to locate the physical collection* and guide users through virtual space in IA. This technology enables to retrieve the documents available. For example, if we want to search any documents by using IoT that connected to the devices, user can get valid and accurate information such as location materials on rack, level and call number.

Information Professionals (IP) also can *help and guide users by providing training and consultant services* on how to use the devices available and how to search information or resources. Therefore, Internet of Things (IoT) technologies make the IA *management process easier and reduce the process of time*.

A study has been conducted by Makori (2017) found some factors that can supports innovation and application of IoT in academic and research IA. The empirical study results indicate that factors responsible for the development of the IoT in the contemporary knowledge economy and society were internet development (95%), computing revolution (95%), globalization (95%), mobile revolution (92%), technological innovation (90%), quality services (89%) and customer needs (85%). Range of IoT technologies applied to heighten access to knowledge and learning in academic

and research IA was explored in this study. Majority of the respondents which is 97% uses digital or electronic information, social media (96%), RFID (95%), mobile platform and cloud computing with 90% respectively and showed that Web of Things (WoT) is on top in the learning in academic and research IA. The findings show that internet, web, hyper connectivity and networking and cloud computing are top influencers the application of IoT in academic and research information organizations.

Respondents also suggested few ideas that IA need to offer in the IoT environment including technology investment (28%), leadership and management (27%), digital information systems (24%) and green movement (21%). Furthermore, findings show the IA should implement leadership programs based on demonstrated potentials and interests, transformation and change and return on investment for customers to have quality and value-added services. To achieve sustainable research and learning goals and practices, the IP should start the deployment of IoT technologies in their organization. The cooperation and trust can encourage improvement and creativity. People can engage in technological and digital initiatives and expand their education, information, knowledge and communication through the collaboration initiative.

### **INTERNET OF THINGS (IoT) IN MALAYSIA**

Although IoT in Malaysia have a slow growth in IoT business, the trend is gradually moving up. In Malaysia, we can see many companies who have taken IoT and implemented it into their businesses to help modernise our local community and bring us towards a digitally integrated lifestyle and workplace. Malaysia Digital Economy Corporation (MDEC) has been one of the key players in expanding the IoT scene in our local community and aimed to position Malaysia as a regional IoT hub. As reported by [Goh Thean Eu](#) in Digital News Asia on Jul 02, 2014 Malaysia has many of the elements of an Internet of Things (IoT) ecosystem but there are challenges need to be resolved before the country can see mass adoption of the technology. The challenges are security, low labor cost, automation and rigid standard operation.

Aligned with IoT growth, MyIoT or Malaysia Internet-of-Things association is founded in 2016 by a group of people in private companies involved in IoT value chain in Malaysia & ASEAN. MyIoT together with industry players are making steps to transformation a successful IoT ecosystem for companies adopting and providing IoT solutions & services.

### **CHALLENGES OF INTERNET OF THINGS (IoT)**

Nowadays, IoT also bring challenges to IA as there are many ways to exploit devices and sources. These issues are still being discussed and debated. IA can be considered as a not for profits organization. Therefore, it is not important to the organizations.

#### *Financial constraints*

Financial constraints are one of the difficult factors to apply IoT in IA because IA need to buy new equipment and devices as well need to train the staff in using technology of IoT. This is because the top management did not see IA as agency that can make profit to organization back. They think that information cannot bring any good to them as they assume that information can be fine just by doing the traditional way. For example, just by asking experience people about the problem they are facing. But in reality, nowadays, most information need to have proof, also need to be show to the right people at the right time and to the right place.

### *Security and Privacy*

In applying IoT, there is an issue on security and privacy. This can consider as serious matter because information can be monopolized greatly to the wrong person. For example, if the wrong person can get personal information regarding his or her personal life, they can be blackmail or maybe threaten in the future. With this situation, it will be bring a lot stress to the person that being blackmail until one day maybe he or she will see suicide will be the only way to escape for the life. For There are three internet securities discuss in [hosting-blog.rackservers.com.au](http://hosting-blog.rackservers.com.au) which are malware, Trojan horses and firewall software.

### *Malware*

Malware refer to worm, spyware and virus which is designed to cause damage to computer or network.

*Worm* will repeat to copy the same data on local drive, network shares and so on. Worm does not harm any data or file in the computer and spread by exploiting vulnerabilities in operating systems. It will take a lot of space in the hard drive and consumes more CPU use that turns computer to be slow and affect users to search the information etc. Anybody can use any devices in IA including computer and may do malicious to get people's confidential information by key logging software that hack computer to get password and personal information. Devices also can be used to send Spams emails to others, store illegal images or overload websites in an extortion attempt by using zombie programs.

*Spyware* programs will collect information about the sites user visit by using IA's computer for advertisers. In using public computer, users need to aware the virus that may attack the computer.

*Virus* will damage or later the file or data in computer as well in devices like external hard disk and pen drive. The data may corrupt or delete by the virus. IoT also bring challenges as nowadays there are many ways that can be exploited.

The IP is still debating on the use of IoT technologies because of this matter. For example, they concern about the user's data will be stolen by the unwanted person like black-hat *hackers*. For IA, data or information is considered as the most assets in the information industry. For the organization, IA is non-profits organization. To organization people, they do not see the potential of IA can become the future. IoT cannot be applied also because of the financial problem. To implement the IoT, IA need to figure out the budget for technologies and also training staff.

Meanwhile, another security issue is tracking a *cookie* which is a plain text file that is stored on computer. Cookies used to track visitor information on website and help the hackers and companies to know personal details like bank account details, credit card information who using the computers. It same goes to misleading applications that misguide users by informing users the computer used is infected by some malware and advice users to download tool to remove the threat. After the tool was download, it will show some threats computer and user need to buy product in order to remove the threat. Users need to disclose personal information like credit card which is can be traced and used by hackers.

### *Trojan Horses*

*Trojan* also one of the security issue in IoT. Trojan is a method for getting malware onto the computer and hidden in other programs that people might choose to download and run. Trojan looks like a genuine application, but they can destructive the computer and open backdoor entry that give



malicious users or programs access to the systems and allow confidential as well as personal information to be theft.

Computer also exposed to virus like *adware* that used by companies for marketing purposes. Adware is a software application that automatically downloaded advertises to the computer. This might interfere users and slow their works.

There are also privacy issues in applying IoT. IA is open space for any users that may use the computer for any purposes. The data that stored in computer may be seen by other users and it lead to *misuse and malicious persons*. For instance, when people use computer to pay bill online, they need to reveal the information like usernames, email address and password. This information may be stored in computer and can be access by anybody. This type of internet vulnerability will make the internet user becomes the target of an online criminal. Most IA also had their own website. IA's website can be access by any individual and the information displays can be used by any parties for their benefits or purposes.

#### *Firewall Software*

All of this security issues will cost the IA to protect their data by buying security tools or product to protect the system as well to hire IT professional. IA also need more time to repair the damage on the computer and it may disturb the service because not all computers can be used at one time and it will give difficulty to the users. Users also connected their devices to the computer's like camera, Smartphone's, external hard disk and pen drive that may have affected from the virus etc. This may lead to the trust issues where the user worried to use the devices in IA and they avoid going to IA.

The issues address above is related to the use of internet and the systems. Therefore, IoT has a potential to disrupt the services. Based on article by Massis (2016), study by HP Security Research in 2014 shows that vulnerabilities will increase when the number of electronic devices and consumer items increase either at home or workplace. The study reveals that more than 25 obvious vulnerabilities identified per device. The devices are such as webcams, home thermostats, remote power outlets, sprinkler controllers, home alarms and garage door openers. It can be concluded that the devices we used every day may help us, but it also may disrupt our lives.

#### *Lack of Expertise for the IoT's technology*

In this era of technology nowadays, most of the people know about the technology but very few people that follow the evolution of the technology. Most of the staffs in IA need to catch up with technology in order to get the latest information and feature from the latest technology. In IA, lack of expertise for IoT's technology brings most of challenge to the agency. This is because, when there are no expert staffs in IoT in the IA, there will be no guide on how to use and also does not the function of that IoT's technology when something happens to the technology. This will bring to the financial matter, because the agency need to send some of their staff to training to make sure that there are expertise in this area. According to Cisco article written by Walker, James (2017), 75 % IoT project failed is due to lack of expertise. Wójcik, M. (2016) also clarify that expertise of IoT is based on three factors that are business skills and technical expertise. Business skill are needed because need to communicate between IT and also business. This skill is needed also because need to make the users understand on how the IoT or that technology work and also need to documentation for the future reference. Technical skill is needed because of need to understand more on IoT technology itself. If anything happen to the technology, these skills are required.

## RECOMMENDATIONS

IoT give variety of benefits to the individuals, businesses and society including IA. It makes life easier as well safe time and cost. However, IoT also had weaknesses as discussed above. Massis (2016) stated that we need to understand four factors that is important which are speed of delivery, platform on which the delivery is accomplished user expectations and trust that the device is verifiable and secure.

While using internet, users expected *speed delivery* and stable platform to do faster works and task accomplished. Users also have high expectations that devices provided are secure in term of security and privacy. Thus, it will provide the users a good image and full trust. IoT also has potential to disrupt the services and role of the IA to alert their users.

### *Transparent Feedback*

If there are vulnerabilities issues arise, IA need to be *more active in providing logical and transparent feedback* to network and device users to ensure that vulnerability issues are fully explained and actions taken by them in addressing the issues. Proper security management explains the need to have proper plan in providing confidence and clear feedback to the user on an ongoing basis. This is also supported by Makori (2017) that a comprehensive, security and control practices must also be put in place to ensure protection of data and information resources.

### *Updated Website*

Another suggestion is IA website must be maintained and updated, so that latest information is available on the website. The descriptive and clarifying statement should be posted on website.

### *Signage*

Signage should be placed in strategic areas which anybody can see and on each public computer which is updated to encourage users to ask the questions. Updated handouts also should be available and social networking platforms to engage with public.

### *Precautions on the Security and Privacy Issues*

In order to build trust from the users, IA needs to take precautions on the security and privacy issues. By using the computer, IA should alert users not to run or open malicious program before download anything to avoid virus infected the computer. Users also need to be advised don't simplify click on the pop-ups that may contain Trojan. To be safe, users must read the terms and conditions before download or agree with any suggestions on the website. IA shall have attached notice at the front desk or noticeboard.

### *Update Antivirus and Firewall*

The computers often vulnerable to the viruses and worms, therefore IA is essential to antivirus updates as well firewall software. Firewall software will stop nasty programs before it's infecting the computer. This method will help to secure the devices and systems safely.

### *Username and Password*

To make sure the IA are safe place to access the computers, IA should put priorities on privacy matters. All computers should have username and password so that people are not easily use the computer without supervision.

### *Cleaning Process*

IA also needs to make cleaning process by configure the settings and clear the browsers that users serve daily. This is important because data or information stored in IA are considered as valuable assets in the information industry. IA normally has their own website. In order to protect data or information in IA, they must set up configurations files either private or can be accessed by public.

### *Advice Users on the Privacy Issues*

IA might advise users on the privacy to ensure their data or information are safe while using computers. Users can protect their data by using passwords and encrypt them to avoid others access the data or information. On top of that, IA alerts users to properly close any programs and sign out any personal internal accounts before leaving the computers. It will protect personal data not visible to the other users.

### *Biometric Scan*

It is recommended that only certain individual can access certain collections such as only IP has the authority. Biometric scan is one of the solution to help IA protect the data or information which is only certain users that been granted by IP can be access to certain collection.

## **CONCLUSION**

IoT has transformed and changed the nature of data, information and knowledge management in IA with innovative technological systems and solutions that have expanded education, learning and competition. Most of information professionals may no longer think that IoT as a factor hindering access to knowledge (Makori, 2017). Therefore, it connects to the networks that create an opportunity to deploy differentiate services either in entertainment like television, data transfer and led to digital society. In the IA, IoT concepts enhance the services in more efficient manner. Besides that, IoT enables IA to reduce the cost, save time and provides the user-friendly system. The technologies that proposed for IoT also can increase profitability by improving resource utilization and development of management services. Smart world of IoT will rapidly increase due to high demand and people are totally depending on IoT in their daily life. Finally, IA also must keep up-to-date to cope with the user's need.

## **REFERENCES**

- Goh, T. U. (2014, December 1). IoT in Malaysia: Challenges ahead before it goes viral. Retrieved from <https://www.digitalnewsasia.com/digital-economy/iot-in-malaysia-challenges-ahead-before-it-goes-viral>
- Goh, T. U. (2015, December 22). MDeC putting the IoT pieces together for Malaysia. Retrieved from <https://www.digitalnewsasia.com/mdec-putting-iot-pieces-together-malaysia>
- Massis, B. (2016). The Internet of Things and its impact on the library. *New Library World*, 117 (3/4), 289-292. doi: 10.1108/nlw-12-2015-0093

Makori, E. O. (2017). Promoting innovation and application of internet of things in academic and research information organizations. *Library Review*, 66 (8/9), 655-678. doi: 10.1108/lr-01-2017-0002

Wójcik, M. (2016). Internet of Things – potential for libraries. *Library Hi Tech*, 34 (2), 404-420. doi: 10.1108/lht-10-2015-0100