INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 2)
Available online at: www.ijariit.com

The Internet of Things: applications and security metrics with the Ugandan perspective

Davis Matovu
davismatovu@yahoo.com
Busitema University, Busia, Uganda

Mugeni Gilbert B.
gbmugeni@gmail.com
Communication Authority of Kenya, Nairobi, Kenya

Karume Simon
smkarume@gmail.com
Laikipia University, Eldoret, Kenya

Mutua Stephen
stephen.makau@gmail.com
Masinde Muliro University of Science and Technology, Kakamega, Kenya

Gilbert Gilibrays Ocen
gilbertocen@gmail.com
Busitema University, Busia, Uganda

ABSTRACT

As the Internet of Things (IoT) increasingly becomes a reality, thousands of devices get connected to IoT platforms in smart cities and regions. These devices will actively send data updates to cloud-based platforms, as part of smart applications in various domains like healthcare, traffic, and education among others. Therefore, it is important to assess the ability of modern IoT systems to handle high rates of data updates coming from devices. The paper aims at developing metrics that can be used to assess the IoT cybersecurity status of a country in terms of the Intensity, Readiness, and Adoption with a special focus of Uganda as a case study. To achieve this, a design science approach was employed. Data were collected from a sample of 127 respondents from 7 firms around Kampala district. Finally, the impact of the proposed metrics is demonstrated through an application to the IoT assessment model.

Keywords— *Internet of Things, Cybersecurity, IoT applications, Metrics*

1. INTRODUCTION

The Internet of Things (IoT; also known as the Internet of Objects) is a system in which the physical world is connected to the Internet through ubiquitous sensors (Victor, 2017). This concept has evolved and extended to several industries and applications over the years, encompassing a vision where networked everyday objects are able to push information, change their state, interact with each other without human intervention and perform actions that affect the physical world (Victor, 2017).

Chen at al. (2014) further asserts that the Internet of Things (IoT) is regarded as a technology and economic wave in the global information industry after the Internet. The IoT is an intelligent network which connects all things to the Internet for the purpose of exchanging information and communicating through the information sensing devices in accordance with agreed protocols (Chen at al, 2014). It achieves the goal of intelligent identifying, locating, tracking, monitoring, and managing things.

According to Chen at al. (2014), IoT should have the following three characteristics;

- **Comprehensive Perception:** Using RFID, sensors, and two-dimensional barcode to obtain the object information at any time and anywhere, it will be a new opportunity.
- **Reliable Transmission:** Through a variety of available radio networks, telecommunication networks, and the Internet, objects information can be available at any time.
- **Intelligent Processing:** By collecting IoT data into databases, various intelligent computing technologies including cloud computing will be able to support IoT data applications. The network service providers can process tens of millions or even billion pieces of messages instantly through cloud computing.

However, as the number of IoT devices continues to increase, so does the number of challenges we face. Security is a big concern since the number of attacks to IoT devices keeps rising. (Bonilla et al, 2017; Teng et al, 2014). It is widely acknowledged that the potential for malicious attacks can and will be greatly spread and actuated from the Internet to the physical word (Teng et al, 2014).

© 2019, www.IJARIIT.com All Rights Reserved

Security of the IoT platform is one of the most important requirements. Security requirements can be identified through an asset–based risk management process in order to describe the security goal.

Various security metrics are used to quantify the degree of freedom from a possibility of suffering damage or loss from a malicious attack (Miroslav et al, 2018). Data quality metrics in pervasive environments can be defined and applied to real-world data sources to demonstrate the feasibility of the metrics.

A subjective user's satisfaction with the application quality of experience, QoE can as well become new quality metrics the operators will have to consider (Miroslav et al, 2018).

Graham (2016) suggests that an IoT threat assessment should include taking stock of the various physical connections, potential losses/impacts, threats and the difficulty of the attack. It is therefore important to address these threats and prioritize them basing on the likelihood and potential impact (Graham, 2016). However, on conducting a security assessment for IoT in Uganda, it was revealed that currently available Security measures for IoT were insufficient to correctly apply to IoT devices and this paved the way for the study.

2. RELATED LITERATURE

2.1 The IoT security

Zhao and Ge (2013) argue that the security issues of the Internet of Things (IoT) are directly related to the wide application of its system starting with introducing the architecture and features of IoT security.

IoT security encompasses several layers of abstraction and a number of dimensions. The abstraction levels range from physical layers of sensors, computation and communication, and devices to the semantic layer in which all collected information is interpreted and processed. It is expected that the majority of security attacks will occur at the software level because it is currently most popular and can simultaneously cover a large number of devices and processes. Thus the need to observe that lowest security at any level and at any dimension so as to determine the overall security (Teng et al, 2014).

2.2 Internet of Things Elements

According to **Al-Fuqaha et al. (2015), u**nderstanding the IoT building blocks helps to gain a better insight into the real meaning and functionality of the IoT. There are six main elements needed to deliver the functionality of the IoT as follows;

2.2.1 Identification: Identification is crucial for the IoT to name and match services with their demand. Many identification methods are available for the IoT such as electronic product codes (EPC) and ubiquitous codes (uCode).

2.2.2 Sensing: The IoT sensing means gathering data from related objects within the network and sending it back to a data warehouse, database, or cloud. The collected data is analyzed to take specific actions based on required services. The IoT sensors can be smart sensors, actuators or wearable sensing devices. For example, companies like Wemo, revolv and SmartThings offer smart hubs and mobile applications that enable people to monitor and control thousands of smart devices and appliances inside buildings using their smartphones.

2.2.3 Communication: IoT communication technologies connect heterogeneous objects together to deliver specific smart services. Typically, the IoT nodes should operate using low power in the presence of lossy and noisy communication links. Examples of communication protocols used for the IoT are Wi-Fi, Bluetooth, IEEE 802.15.4, Z-wave, and LTE-Advanced. Some specific communication technologies are also in use like RFID, Near Field Communication (NFC) and ultra-wide bandwidth (UWB). Other communication technologies are Wi-Fi that uses radio waves to exchange data amongst things within 100 m range and LTE (Long-Term Evolution) is originally a standard wireless communication for high-speed data transfer between mobile phones based on GSM/UMTS network technologies.

2.2.4 Computation: Processing units (e.g., microcontrollers, microprocessors, SOCs, FPGAs) and software applications represent the "brain" and the computational ability of the IoT. Various hardware platforms were developed to run IoT applications such as Arduino, UDOO, Friendly ARM, Intel Galileo, Raspberry PI, Gadgeteer, BeagleBone, Cubieboard, Z1, WiSense, Mulle, and T-Mote Sky.

Furthermore, many software platforms are utilized to provide IoT functionalities. Among these platforms, Operating Systems are vital since they run for the whole activation time of a device. There are several Real-Time Operating Systems (RTOS) that are good candidates for the development of RTOS-based IoT applications. Cloud Platforms form another important computational part of the IoT. These platforms provide facilities for smart objects to send their data to the cloud, for big data to be processed in real-time, and eventually for end-users to benefit from the knowledge extracted from the collected big data.

2.2.5 Services: Overall, IoT services can be categorized under four classes: Identity-related Services, Information Aggregation Services, Collaborative-Aware Services and Ubiquitous Services. Identity-related services are the most basic and important services that are used in other types of services. Collaborative-Aware Services act on top of Information Aggregation Services and use the obtained data to make a decision and react accordingly. Ubiquitous Services, however, aim to provide Collaborative-Aware Services anytime they are needed to anyone who needs them anywhere. With this categorization, we review some applications of the IoT in the following paragraphs. The ultimate goal of all IoT applications is to reach the level of ubiquitous services.

© 2019, www.IJARIIT.com All Rights Reserved

2.2.6 Semantics: Semantic in the IoT refers to the ability to extract knowledge smartly by different machines to provide the required services. Knowledge extraction includes discovering and using resources and modelling information. Also, it includes recognizing and analyzing data to make sense of the right decision to provide the exact service.

2.3 Cyber risk assessment in the Internet of Things domain

According to Radanliev et al (2018), cyber risk assessment requires categorising into (1) risk identification assessment strategy; (2) risk estimation strategy; and (3) risk prioritisation strategy. This because IoT capabilities create new types of cyber risk, which are neither anticipated nor considered in existing cyber risk assessment standards. Radanliev et al (2018) further argue that integrating IoT technology in the communications networks of critical infrastructure implies major ethical aspects that humans should be able to be aware of and comprehend, while also benefiting from maximum possible levels of trust and privacy. Integrating IoT technology in the communications networks also triggers question on data ownership, data privacy and economic lifespan of digital assets (Radanliev et al, 2018).

3. METHODOLOGY

The study was carried out in Kampala district, Uganda. Using Krejcie and Morgan table, (1970), a sample of 127 respondents from 7 firms (The Ministry of ICT of Uganda, National Information Technology Authority of Uganda, Uganda Communication Commission, Security Agencies of Uganda and Universities.) were conveniently selected based on their accessibility and willingness to participate. It also gave each respondent an equal chance of being selected to participate in the study (Mugenda and Mugenda, 1999).

Purposive sampling permits selecting key informants who are knowledgeable about the situation (Amin, 2005). The study also used purposive sampling to select all Technical staff of the Cyber Security Unit and Emerging Technologies in each of these firms due to the need to target respondents who are knowledgeable on required information.

Primary data was collected using questionnaires and interview guides in focus groups. Secondary data was collected through documentary analysis. Secondary data sources include; previous researches and analyses of scholars; books, Journals, Conference proceedings, white papers and Government publications on cybersecurity that are related to the current trend of cyber emerging threats.

These mainly were composed of closed-ended questionnaires to the respondents. The closed-ended questionnaires form is advantageous in that it will be easy to fill out, saves time and keeps respondents on the subject and relatively objective. The questionnaire used a 5-point Likert scale ranging from 5 (strongly agree) to 1 (strongly disagree), in order to provide consistent responses. The questionnaire was designed to establish the extent of the respondents' agreement with the statements. The questionnaire was preferred because it's a quick way in data collection and it's easy to categorize, Quantify and generalize information.

Reliability and validity of the instrument were tested. Reliability refers to the consistency of a test, survey, observation, or other measuring instruments and describes the extent to which instruments will produce consistent results in similar conditions over time (Holmström et al., 2009). Validity refers to the credibility and/or dependability of the research results (Salat&Dillman, 1994). In order to ensure validity, the researcher employed several methods including triangulation of data obtained via different research instruments and review, prolonged engagement with respondents. (Holmström et al., 2009).

Accordingly, a pilot study to pretest the questionnaire was conducted using 5 respondents randomly selected from the target respondents with similar characteristics as the target population but who were not to participate in the final survey. The instrument was also discussed with content experts suggested by the supervisors in the field of IoT cybersecurity. The experts were specifically requested to indicate whether the items in particular sections of the questionnaire adequately measured the respective constructs and whether the instrument was appropriate for this kind of study. The final instrument was developed upon incorporating all comments from the experts.

Assessment instruments must be both reliable and valid for study results to be credible. In the present study, the reliability of the assessment tool was estimated using Cronbach alpha test of internal consistency. This test is frequently used to calculate the correlation values among the answers in the assessment tool. Cronbach alpha calculates correlation among all the variables, in every combination; a high-reliability estimate should be as close to 1 as possible. The results are presented in Table 1.

Table 1: Results

Variable	Number of items	Cronbach's Alpha value
IoT threats exposure	9	.934
Risk determination of IoT	27	.968

Source: Primary Data

As shown in Table 1, all variables in the study a Cronbach alpha reliability coefficient above the acceptable minimum of 0.50 (Cronbach, 1951; Nunnally, 1978; Sekaran, 2000). This indicates that the instrument used to collect data in this study was acceptable.

Data obtained from close-ended responses were verified, processed and analyzed using the descriptive and inferential statistical analysis using SPSS version 16.0. The results are presented in the next section 4.

© 2019, www.IJARIIT.com All Rights Reserved

4. RESULTS AND DISCUSSIONS

4.1 Description of Statistics

The demographic characteristics of the respondents analyzed include gender, age, level of education and experience working at the job in Uganda. Results of the demographic characteristics of the sample studied are presented using frequency tables.

Table 2: Descriptive characteristics of the respondents

Variable (N=127)	Description	Frequency	Percent
Gender	Male	74	58.3
	Female	53	41.7
Age	18-34years	40	31.5
	35-44years	42	33.1
	45-54years	32	25.2
	Above 55years	13	10.2
Education level	Diploma	19	15.0
	Degree	40	31.5
	Masters	68	53.5
Experience	<5years	39	30.7
	5-10 years	39	30.7
	10-15 years	30	23.6
	Above 15years	19	15.0

Source: Primary Data

Regarding the background characteristics of the respondents, table 1 indicates that the study was male-dominated because, out of the 127 respondents constituting a percentage of (58.3%), 74 were males while 53 were females. It also revealed that most of the respondents (33.1%) were in the age bracket of 35-44years; followed by (31.5%) who were in the age bracket of 18-34years,this was followed by (25.2%) who were in the age bracket of 45-54years, and the least percentage (10.2%) were above 55 years.

Regarding the respondents' education level was such that the biggest percentage (68.0%) had above a master's degree, which implies that they could articulately read and understand the questions posed in that questionnaire, followed by degree holders (40%), and diploma holders (15.0%).

Regarding the respondents' experience, the study revealed that the majority of respondents (30.7%) had work experience in the field of cybersecurity of 5 to 10 years, this was followed by (30.7%) who had an experience of less than 5years. (23.6%) of the respondents had a work experience of 10 to 15 years and (15.0%) had a working experience of above 15years in the field of cybersecurity.

4.2 (IOT) Internet of Things cyber threats exposure In Uganda

Descriptive analysis was conducted on the items measuring IoT cyber threats Exposure to examine the level of IoT cyber threats Exposure in Uganda. On a scale of 1 = "No exposure" , implying a low IoT cyber threats Exposure to 5 = "Extremely exposed", implying high IoT cyber threats Exposure. The results are presented in Table 3.

Table 3: Descriptive statistics of IoT cyber threats Exposure in Uganda

Measurement items	N	Mean	S.D
IoT cyber threats Exposure			
Denial-of-service attacks	127	1.61	1.027
Data espionage	127	1.90	.970
Natural threats	127	1.80	.988
Sabotage	127	1.90	1.050
Computer Frauds	127	1.90	1.113
Malicious attacks	127	1.91	1.088
Message falsification or injection	127	1.98	1.058
Vandalism	127	1.94	1.098
Copyright Violations	127	1.78	1.080

Source: Primary Data

4.3 Factors that determine the internet of things risks in the domain of readiness

Descriptive analysis was conducted on the items measuring Factors that determine the internet of things risks in the domain of readiness in Uganda. On a scale of 1 (strongly disagree) to 5 (strongly agree), mean values less than 2.50 were interpreted as depicting a high readiness. On the other hand, mean values of 2.50 or more depicted low readiness. The results are presented in Table 4.

Table 4: Results

Measurement items	N	Mean	S.D
Policy (PO)			
There is an IoT Cyber Security Policy, and the policy achieves its intended purpose	127	2.40	1.393
There is the existence of a functioning Cyber Security department in my Organization	127	2.57	1.551
There are systematic administrative procedures for gathering information regarding IoT risks	127	2.62	1.431
Mean		**2.53**	

© 2019, www.IJARIIT.com All Rights Reserved

Human Resource (HR)			
There is the availability of cybersecurity trained technical personnel in my organization	127	2.85	1.633
There are documentation and monitoring of the privacy and security training activities for employees in the organisation.	127	2.86	1.361
The organization conducts employee IoT Security awareness and education campaigns.	127	3.01	1.354
Cybersecurity roles and responsibilities for all staff are established in my organisation.	127	2.96	1.461
Mean		**2.92**	
Infrastructure (IN)- Demand side infrastructure			
There is infrastructure for monitoring and detecting cybersecurity threats in my organization	127	2.94	1.388
My organisation has information risk and security management tools.	127	2.92	1.395
My organisation has an incident response plan in place in the event of a breach.	127	2.98	1.586
Mean		**2.94**	
Infrastructure (IN)- Supply side infrastructure			
My organisation verifies that the IoT hardware and software acquired performs as expected and their overall security posture is as per the organisational standard.	127	3.17	1.473
The organisation IT security experts are always engaged in the IoT software and hardware preliminary tests with the suppliers before final delivery of the products.	127	3.31	1.417
Mean		**3.24**	
Grand mean		**2.91**	

Source: Primary Data

As shown in Table 4, the grand mean for factors that determine the internet of things risks in the domain of readiness in Uganda was 2.91 suggesting that; overall, the expatriates working in the firms surveyed perceived a high similarity between the readiness. A high similarity among readiness implies the existence of low readiness among the expatriates and local operating environment. This low readiness was attributable to a low policy (mean = 2.53) coupled with high human resources (mean = 2.92). However, there was a high level of infrastructure (in)- supply-side infrastructure (mean = 3.24) in the organizations surveyed.

4.4 Factors that determine the internet of things risks in the domain of intensity

Descriptive analysis was conducted on the items measuring Factors that determine the internet of things risks in the domain of intensity in Uganda. On a scale of 1 (strongly disagree) to 5 (strongly agree), mean values less than 2.50 were interpreted as depicting a high intensity. On the other hand, mean values of 2.50 or more depicted low intensity. The results are presented in Table 5.

Table 5: Results

Measurement items	N	Mean	S.D
Awareness (AW)			
There is an IoT Cyber Security Policy, and the policy achieves its intended purpose	127	3.29	1.392
There is the existence of a functioning Cyber Security department in my Organization	127	3.22	1.532
We regularly train staff to make them aware of IoT cybersecurity risks in the organisation.	127	3.54	1.557
Mean		**3.35**	
Severity and Impact(SI)			
I understand the need to safeguard personal information from unlawful access	127	4.05	1.240
Any personal data online or on an IoT device is treated as confidential and cannot be disclosed without one's consent.	127	3.76	1.355
There is an accounting mechanism to determine the effect of IoT cybercrime	127	3.59	1.293
Mean		**3.80**	
Grand mean		**3.57**	

Source: Primary Data

As shown in Table 5, the factors that determine the internet of things risks in the domain of intensity surveyed in Uganda was high (Grand mean = 3.57). This high level of intensity was attributed by severity and impact (mean = 3.80). On the other hand, the results indicate that awareness was modest (mean = 3.35).

4.5 Factors that determine the internet of things risks in the domain of adoption

Descriptive analysis was conducted on the items measuring Factors that determine the internet of things risks in the domain of adoption in Uganda. On a scale of 1 (strongly disagree) to 5 (strongly agree), mean values less than 2.50 were interpreted as depicting a high adoption. On the other hand, mean values of 2.50 or more depicted low adoption. The results are presented in Table 6.

Table 6: Results

Measurement items	N	Mean	S.D
Privacy and Security (PS)			
I am satisfied with the inherent security built in commonly available IoT devices and networks	127	1.61	1.025
The effect and impact of IoT cybercrime rate is evaluated at my organization	127	1.89	.970
There is a department to manage the IoT cyber threats and risks at my organization	127	1.80	.987
Mean		**1.77**	
Self Efficacy (SE)			
I have the necessary skills to handle common IoT security risks	127	1.94	1.049

© 2019, www.IJARIIT.com All Rights Reserved

I have the knowledge to identify and address potential IoT cyber security risks for users and providers than our competitors	127	1.90	1.112
I am aware of the fundamental standards that make it possible to create flexible strategies for the protection of organisational IoT devices and applications against IoT cyber security risks.	127	1.91	1.087
Mean		**1.92**	
Facilitating Conditions (FC)			
We have technological skills and competencies in the organization for increased protection and security against the IoT cyber security risks.	127	1.98	1.058
We have the in-house expertise to help in adoption, of security controls and monitoring of IoT cyber security risks in the organisation.	127	1.94	1.097
The organization has financial resources to put in place the infrastructure needed to secure against IoT cyber security risks and threats	127	1.77	1.078
Mean		**1.89**	
Grand mean		**1.86**	

Source: Primary Data

As indicated in Table 6, the overall, the level of Factors that determine the internet of things risks in the domain of adoption surveyed in Uganda was low (Grand mean = 1.86). This level of performance is majorly attributed to low satisfaction with the inherent security built in commonly available IoT devices and networks (mean = 1.61, S.D = 1.025) and limited financial resources to put in place the infrastructure needed to secure against IoT cybersecurity risks and threats (mean = 1.77, S.D = 1.078). Others include the effect and impact of IoT cybercrime rate is not being efficiently evaluated (mean = 1.89, S.D = .970) and absence of a department to manage the IoT cyber threats and risks at mean = 1.80, S.D = .987).

5. CONCLUSION

Cyber security is a new area of research that has rapidly attracted attention in the government, Technology industry and academia. The aim of this survey is to assess the state of IoT in Uganda and derive metrics for assessing IoT. The results reveal various assessment metrics under different domains as seen below;

Assessment metrics such as facilitating conditions, self-efficacy, privacy and security are used to assess the factors under the domain of readiness. Furthermore, Assessment metrics such as severity and impact, awareness, human resource are used to assess the factors under the domain of intensity and lastly the metrics of infrastructure (in)-demand side and supply side, policy are used to assess the factors under the domain of adoption.

This study, therefore, recommends that governments and IT industry globally should be wary of the growing danger of IoT security in the near future and better improvise efficient and secure implementation of IoT technologies.

6. REFERENCES

[1] Treffyn L, K., Toni, R., Tuck W, L.(2013)Internet of Things: a review of literature and products.Conference Paper · ACM 978-1-4503-2525-7/13.DOI: 10.1145/2541016.2541048.

[2] Krejcie, R.V., & Morgan, D. W (1970). Determining Sample Sizes for Research Activities, Educational and Psychological Measurements, 30,608.

[3] Von Solms, R, Niekerk, J.(2013)From information security to cyber security. computers & security38(2013) 97 e102. Elsevier Ltd

[4] Ralstona, P.A.S., Grahamb, J.H., Hiebb, J.L.(2007)Cyber security risk assessment for SCADA and DCS networks. ISA Transactions 46 (2007) 583–594.

[5] Salant, P.&Dillman, A. (1994). How to conduct your own survey. John Wiley & Sons, Inc 1994

[6] Holmström, J., Ketokivi, M., &Hameri, A. (2009). Bridging Practice and Theory: A John Wiley & Sons, Inc (2009).Design Science Approach to bridging Practice and Theory

[7] Amin, M.E. (2005). Social Science Research, Conception, Methodology Analysis. Kampala: Makerere University Printery.

[8] Ollie white house (2015), An Implementer's Guide to Cyber-Security for the Internet of Things Devices and Beyond.

[9] Radanliev, P., Charles De Roure, D., Nicolescu, R., Huth, M., Mantilla Montalvo, R., Cannady, S., Burnap, P.(2018).Future developments in cyber risk assessment for the internet of things. Computers in Industry 102 (2018) 14–22

[10] R. I. Bonilla, J. J. Crow, L. S. Basantes and L. G. Cruz, "A Metric for Measuring IoT Devices Security Levels," 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), Orlando, FL, 2017, pp. 704-709.Accessed from

[11] URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8328467&isnumber=8328301

[12] Graham, B.(2016).First Things First: Threat Analysis and Assessment for IoT Devices. Accessed from https://www.iotcentral.io/blog/first-things-first-threat-analysis-and-assessment-for-iot-devices

[13] Zhao, K & Ge, L. (2013). A Survey on the Internet of Things Security. Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013. 663-667. 10.1109/CIS.2013.145.

[14] Teng, X., James, B. Wendt, and Miodrag Potkonjak(2014).Security of IoT Systems: Design Challenges and Opportunities. IEEE

[15] Chen, S., Xu, H., Liu, D., Hu, B. and Wang, H. (2014)."A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective," in IEEE Internet of Things Journal, vol. 1, no. 4, pp. 349-359.

[16] Miroslav, B., Xavier, B., Karel, F and Bestoun, S.A.(2018). A Comprehensive View on Quality Characteristics of IoT Solutions. Urb-IoT 2018.3rd EAI International Conference on IoT in Urban Space, Guimares, Portugal.

© 2019, www.IJARIIT.com All Rights Reserved

[17] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M. (2015)"Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp.

© 2019, www.IJARIIT.com All Rights Reserved