ECONSPEAK: A Journal of Advances in Management IT & Social Sciences,
Vol. 9, Issue 7, July 2019 Impact Factor 6.569 ISSN: (2231-4571)
www.skirec.org Email Id: skirec.org@gmail.com

INTERNET OF THINGS AND USER PRIVACY

Paluku Kazimoto & Edwardson Pedragosa Jr.

ABSTRACT

This paper explores how Internet of things (IoT) affect individual space and privacy. The purpose of the study was to describe and explain what involves for the internet of things affecting security and privacy. The quantitative methods such as the Pearson correlation coefficient and multiple regression were used for data analysis from 50 participants selected purposely for data collection. Results reveal that there is positive statistically significant relationship between internet of things and user privacy. The results show that the higher the use of devices, network connections, data transfer, the cyberattacks and application of technology regulations the higher the need of users' privacy. Using Regression Analysis findings show that any change in the device and cyberattacks (ad R Square= .951) affects the level of user privacy for using internet of things. Coefficients for the regression model findings show that independent variables at each 1 unit of increase, the devices for communication has an increase of 0.555 and cyberattacks of 0.310 respectively affecting the user privacy. The findings were confirmed by the analysis for Pearson correlation coefficient that indicated the higher and positive significant relationship between Internet of things (IoT) and user's privacy. Therefore, there is more concerns from participants about the data security and the privacy invasion by the Internet of things. Thus, most of the participants recommended that there is a need to have effective regulations and policies to protect them from any invasion of their privacy and security of the information from Internet of things.

KEYWORDS: Networking, Internet of things, user's privacy, data and information security

INTRODUCTION

BACKGROUND OF THE STUDY

Today's technological advancement in the world provides benefits to society and organizations communication for data and information sharing. In a dynamic social technology, individuals are accessing information and are able to communicate between themselves. These are facilitated through internet, varying devices, people that make Internet of things possible. The development of technology faces more advancement for information sharing between users that creates challenges for security and privacy of data and information. Whether people like it or not, technological

changes is on-going. With the new technology that are part of Internet of things transmission of information and data from machine to machine is accessible. Sensing, interaction, and control of information become even more sophisticated (Stankovic, 2014). There seems to be a significant overlap for the communities with sometimes slightly different perspectives for the use of Internet of things.

The concept of the Internet of things (IoT) aims to make the Internet more immersive and pervasive for communication; enabling easy access and interaction with a wide variety of devices (home appliances, surveillance cameras, monitoring sensors, actuators, displays, vehicles, etc). The IoT is not only for people interaction but also is applied in many other different domains (home automation, industrial automation, medical aids, healthcare, elderly assistance, intelligent energy management and smart grids, automotive traffic management, etc.) (Zanella, Bui, Vangelista & Zorzi, 2014).

With this new technology, Køien (2015) found a recent rapid development of the Internet of things (IoT) that is its ability to offer different types of services with a massive impact on social life and business environments. For Gartner (2015), the future of the IoT will exponentially boom, increasing the trend of billions of people connected to the internet, and the number of connected devices to exceed 50 billion by the year 2020. The Internet of things (IoT) shows a significant transformation in a digital world that ever happened but this will potentially affect people's privacy and security in terms of data and information.

With the growth of technology, the Internet of things (IoT) attracts people to connect devices for data and information sharing. The security of data and information becomes a significant concern that is a potential risk for people's privacy. Businesses are increasingly being breached by attackers (Carlson, Creighton, Meyer, Montgomery & Reiter, 2014). Rajpoot, Vashney & Nailwal (2016). mentioned that the significant difference between the traditional Internet and the IoT is the amount of data and information being collected about the user without his/her knowledge.

Technology has changed the way communication of data and information is transmitted between people to machine and machine to people. Data transfer via computer to machine and from devices to the cloud have helped the transmission of data more efficiently and effectively. However, people have doubts about the security of their information and transfer of data and information. The security of data and information becomes the significant concern of users. Although there are regulations and policies for communications, there is less concerning security of data and information transfer, use of devices, etc. For the IoT users, there seems to be more attack and

stealing of sensitive information. This study aims to investigate the factors of Internet of things and user's privacy for communication.

- What are the factors that affect users 'privacy on the Internet of things system?
- At which extent is the user's privacy from the use of Internet of things?
- Is there significant effect of factors of the Internet of things on the user's privacy?

LITERATURE REVIEW

The organization's managers are to be sensitive about data and information security. Using and keeping up to date with new technology have affected the users and machines to communicate with each other and increased the chance of losing data. As cybersecurity, where the Internet of things differ from user communities, Velosa (2013) stated that the value of Internet of things implementations in cities lies in the huge amount of big data they generate and information policies to address privacy and citizen value are to be taken into consideration by chief information officers

Afshar (2017) reported that Boston Consulting Group (BCG), B2B spending on Internet of things (IoT) technologies, apps and solutions will reach $267B by 2020, with 50% of IoT spending will be driven by discrete manufacturing, transportation and logistics, and utilities. Empathizing on the user's perspective, more responsive policy approaches helps to calibrate guidance and requirements to address security concerns without limiting IoT innovation adequately. The Internet of things will be transformative in its generation of new business opportunities and its impact on IT (Nguyen, 2016). A coherent Internet of things strategy is key to the success of an organization's digital business transformation. Successful implementation and management of that strategy involve both new technical and organizational know-how (Hung, 2018).

Barcena & Wueest (2015) stated that most proposed IoT attacks are proofs-of-concept and have generated income for people. As the company stakeholders invest time and money in a stable security structure, the focus of managers was to be on the most common attacks, and regular training to the staff as priority. The threats likely don't spare users for their data and information. To protect the privacy of clients in the form of increased security for authentication for any attempt into the system can be as important for users. CableLabs (2017) indicated that insecure IoT devices pose a risk to both consumers and the basic functionality of the Internet. These risks continue to increase based on organic technology and market trends that are making IoT security a growing problem. Most prominently, connected devices are proliferating in the home as broadband capacity grows.

Authentication prevent threats and protect privacy of users and security of the Internet of things is essential to be put in place. Security can be established to protect privacy and facilitate the

collection of large amounts of data. There are risks to security flow from the Internet of things. Those risks may involve the direct collection of sensitive personal information, data, locations, and physical conditions over time. Friedman & Heudecker (2015) reported there impacts the IoT have on information management:

- Analytics of the data and the devices that generate data are highly distributed in an IoT architecture,
- Stakeholder relationships in the IoT are complicated and multifaceted, while data ownership and usage rights can be vague and highly dynamic, making information governance a big challenge for information managers
- A range of analytical time frames, from real time to batch, are required for IoT use cases, impacting not just infrastructure but also people and business processes

In February 2016, the USA Chamber of Commerce and the Federal Trade Commission focused on the importance of having self-regulation and security frameworks that aren't overly rigid. Organizations were to design and develop new regulations and standards for IoT and data-privacy to guide companies, devices and users to prevent cyber-attacks (Andrews, El-Attrash, & Chakrabarty, 2016). The exponentially growing number of cyber-attacks from one computer to another or through networks is a failure from inside system control. Marianne (2018) stated that cyber-attack involves hackers, virus, malware, phishing, and other activities from the computer operations. Attacks can come from within or outside an organization system.

In 2017, cyber-attacks had the goal to disable the target computer and knock it offline to get access to the target company computer's data systems. Investigators reported that the motive of cyber-attacks ranged from pure profit to disruption and political pressure organized by crime gangs and hackers (Dearden, 2017). Generally, small businesses are more vulnerable than large companies because of fewer or lack of resources to devote to security, where big businesses find it difficult in addressing cybersecurity (Karisny, 2015).

IoT demands a technical strategy for its implementation in organizations (Heidt (2018) and Zlotogorski, Stevens & Johnson (2019) report showed that Emerging 5G networks represent a key enabler for digital business and Internet of things strategies. Information managers need to familiarize themselves for the introduction of 5G and the future disruption that it represents across the end-to-end supply chain.

Cisco's network growth forecasts based on greater adoption of mobile, wireless and IoT technologies show that by 2021, global IP traffic will reach 3.3 Zetabyte per year. Smartphones will account for 33 percent of total IP traffic. Traffic from wireless and mobile devices will account for more than 63

percent of total IP. Wired devices will account for 37 percent of IP traffic, while Wi-Fi and mobile devices will account for 63 percent of IP traffic. The number of devices connected to IP networks will be three times as high as the global population. There will be 3.5 million networked devices per capita, broadband speeds will nearly double, and global fixed broadband speeds will reach 53.0 Mbps, up from 27.5 Mbps in 2016. Users will be more exposed while using Internet of things by 2021 (Afshar, 2017).

Lee and Kobsa (2017) found that the Internet of things (IoT) users would like to have privacy and keep their personal information. Today the internet has advanced considerably to support communication through multimedia traffic, using telephone, music, and social media. The Internet has facilitated users to access a variety of information stored at different sites (Kharagpur, 2017). Lee and Kobsa (2016) stated that the users' privacy in practice is likely to develop explosion of sensor devices for the future of the Internet of things. Psychoula, Singh, Chen, Chen, Holzinger, and Ning, (2018) find that many people need to make decision to the offered Internet of things services unless they found them useful and practical for their daily lives without interfering with their privacy.

METHODOLOGY

The purpose of the study was to describe and explain what involves for the Internet of things affecting security and privacy. The study used quantitative methods such as the Pearson correlation coefficient and multiple regression for data analysis from 50 participants selected purposely for data collection. The target population was formed by students and faculty from a University. They were selected based on their work environment as users of Internet of things to find out about their awareness about security for their privacy.

The researcher purposely selected 65 respondents to participate into the study. Only 50 respondents were able to fill the questionnaire and participated in the study. The findings reveal that slightly above half (52.0%) of participants were male and 48.0% of them were female. More than half (60.0%) of participants represented those aged above 21 years old and others (40.0%) were aged 21 years old. Data were analyzed using descriptive statistics such mean and percentages to have the participants opinions on the statements formulated in the questionnaire. The following measurement scales were used to interpret the Mean of <1. Strongly disagree; 1.1 – 1.95= Disagree; 1.96-2.85=Neutral; 2.76-3.55 = Agree and above 3.56 = Strongly Agree. Pearson correlation coefficient and multiple regression analysis were done to find out the significance of IoT on the users' privacy for data and information.

FINDINGS AND DISCUSSIONS

Internet of things (IoT) devices usage

Descriptive statistics were used to analyze the data from respondents on the Internet of things devices and awareness about it.

Table 1. : Internet of things devices usage

How often do you use Internet of things		n	%
	Always	31	62.0
	Often	14	28.0
	Sometimes	4	8.0
	Never	1	2.0
Awareness about IoT			
	Always	20	40.0
	Often	13	26.0
	Sometimes	12	24.0
	Never	5	10.0

T

The results in table 1 show that most (62%) of participants always use the Internet of things' devices, 28.0% often used IoT devices, 8.0% sometimes and only 2.0% never used IoT devices. In line with the results, Afshar (2017) reported that Boston Consulting Group (BCG), B2B spending on Internet of things (IoT) technologies, apps and solutions will reach $267B by 2020, with 50% of IoT spending will be driven by discrete manufacturing, transportation and logistics, and utilities. The findings show that slightly less than half (40.0%) of participants always were aware about IoT usage, 26.0% often 24.0% sometimes and only 10.0% they never heard about it.

User Privacy

The descriptive statistics were used to analyze the responses for each item on security and privacy of users. Each item was described based on a 5-point scale option, Mean of <1. Strongly disagree; 1.1 – 1.95= Disagree; 1.96-2.85=Neutral; 2.76-3.55 = Agree and above 3.56 = Strongly Agree

Table 2. : *User Privacy*

Privacy	Mean	SD	Decision
I'm concerned that my information may be transmitted over internet and/or stolen.	3.46	0.86	Agree
I would like to know everyone who is collecting data about me and what they are doing with it	3.88	0.80	Strongly Agree
I'm concerned more about convenience for my privacy	3.94	0.98	Strongly Agree

Findings in table 2 indicate that most (mean=3.94) of respondents strongly agreed to be concerned about their privacy and concerned about information collected from them (Mean=3.88), others (Mean=3.46) agree to be concerned about how information is being transmitted via internet.

Internet of things (IoT)

The descriptive statistics were used to analyze the responses for each item on security and privacy of users. Each item was described based on a 5-point scale option, Mean of <1. Strongly disagree; 1.1 – 1.95= Disagree; 1.96-2.85=Neutral; 2.76-3.55 = Agree and above 3.56 = Strongly Agree

Table 3. : *Cyber-attack using Internet of things*

Cyber attack	Mean	SD	Decision
I update my antivirus regularly	3.00	1.21	Agree
Small businesses are safer from cyber-attack compared to big banks and big companies	3.12	1.00	Agree
Security threats are too complicated for me to understand	3.40	1.06	Agree
I've encountered problems in the past 12 months unauthorized access and leak of personal information, and infected with virus.	3.00	1.03	Agree

Findings in table 3 show that the respondents agreed on the fact that security attacks are too complicated as compared to small business that are safer that large businesses. Although, those respondents agree to have been updating their antivirus regularly, however, for the past 12 months they have encountered problems of unauthorized access to personal information and system interrupted by virus.

Table 4.: *Regulation of Internet of things*

Regulation	Mean	SD	Decision
Internet of things needs specific regulation on technology devices connection	3.84	0.98	Strongly Agree
I'm aware of technology policies	3.44	1.01	Agree
I need to know about the privacy practices regulations	3.66	0.89	Strongly Agree
Communication between devices			
My devices are connected with each other (eg: laptop and phone)	3.68	1.10	Strongly Agree
Device communication makes my life easier	4.06	0.84	Strongly Agree
It's annoying when it sends notification to more than one	3.62	0.88	Strongly Agree

device.

Communication Network			
My devices are interconnected via wireless and cables	3.66	1.08	Strongly Agree
My current Internet connection speed is meeting my current needs for personal and professional use	3.66	0.94	Strongly Agree
The price I'm paying for the communication is affordable	3.52	0.86	Agree
Data Transfer			Strongly Agree
I prefer to ensure my data transfer to be encrypted	3.66	0.89	Strongly Agree
I normally need to transfer large size of data to other devices (video)	3.46	0.99	Agree
Speed is very important for me in transferring my data.	3.94	0.93	Strongly Agree

Results in table 4 reveal that majority (Mean of 3.84 and Mean of 3.66) strongly agreed that there is a need to reinforce regulation on technology and know more about privacies regulations, and other respondents (Mean=3.44) agreed to be aware and know technology policies. Respondents strongly agreed (Mean=4.06). to have been connecting all their devices with each other to easy their communication. Regarding networking, participants agreed that they have been connecting devices via wireless and cables, satisfied with the speed for their connection for their devices that is affordable. Results show that respondents strongly agreed and commented to have good speed to transfer data (Mean=3.94), but that they need encryption to transfer their data (Mean=3.66) and agreed that they always transfer large data from their devices (Mean=3.46).

Correlation Analysis between Internet of things and User Privacy

Pearson correlation coefficient was used to examine the relationship between factors of Internet of things and user privacy. Results in table 4 reveal that there is positive statistically significant relationship between Devices for communication (r=.970), Data Transfer (r=.963), Technology regulations (r=.962), Cyber-attacks (r=.961), network for interconnections (r=.958) and user privacy. In general, the result show that the higher the use of devices, network connections, data transfer, the presence of Cyberattacks and application of technology regulations the higher the need for privacy. Therefore, the null hypothesis is accepted that there is a very significant correlation between Internet of things factors and user privacy.

Table 5.: *Correlation Analysis between Internet of things and User Privacy*

		Privacy
Cyberattacks	Pearson Correlation	.961**
Technology Regulations	Pearson Correlation	.962**
Device for Communication	Pearson Correlation	.970**
Network for Interconnections	Pearson Correlation	.958**
Data Transfer	Pearson Correlation	.963**

Regression Analysis of factors for Internet of things and User Privacy

On the other hand, linear Regression Analysis using stepwise method was used to identify the factors that are highly affecting the privacy of respondents. Findings in table 5 show that any change in the device and cyberattacks (ad R Square= .951) affects the level of user privacy for using Internet

Table 6: *Model Summary*

				Std. Error	Change Statistics				
Model	R	R Square	Adjusted R Square	of the Estimate	R Square Change	F Change	df1	df2	Sig. F Change
1	.970[a]	.941	.940	.20482	.941	762.665	1	48	.000
2	.976[b]	.953	.951	.18468	.012	12.041	1	47	.001

a. Predictors: (Constant), Device Communication

b. Predictors: (Constant), Device Communication, Cyberattacks

of things.

The ANOVA analysis in table 6 show that there is very significant difference between the means of factors of Internet of things and user privacy with *p* value = .000. The findings show that the main factors that have difference in affecting user privacy are the devices for communication and the cyber-attacks. The F-test shows that there is significant variance between the predictors for the user

Table 6: *ANOVA*[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	31.995	1	31.995	762.665	.000[b]
	Residual	2.014	48	.042		
	Total	34.009	49			
2	Regression	32.406	2	16.203	475.066	.000[c]
	Residual	1.603	47	.034		
	Total	34.009	49			

a. Dependent Variable: Privacy

b. Predictors: (Constant), Device Communication

c. Predictors: (Constant), Device Communication, Cyberattacks

From table 7 of coefficients for the regression model show the analysis of the stepwise methods that indicate how the changes in each independent variable affect the dependent variable. From the column of the unstandardized coefficients, the beta coefficient indicates the degree of change in the outcome variable for every 1-unit of change in the predictor variable. The findings show that independent variables; devices for communication with beta value of 0.900, indicate that for each 1 unit in this predictor there is an increase of 0.900 in user privacy. From the analysis of both predictors, 1 unit increase for the devices for communication there is an increase of 0.555 and for 1 unit increase in cyber-attacks there is an increase of 0.310 for the user concern on privacy.

Table 7: Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	.352	.127		2.778	.008
	Device Communication	.900	.033	.970	27.616	.000
2	(Constant)	.686	.149		4.591	.000
	Device Communication	.555	.104	.598	5.359	.000
	Cyberattacks	.310	.089	.387	3.470	.001

a. Dependent Variable: Privacy

DISCUSSION AND CONCLUSION

Pearson correlation coefficient was used to examine the relationship between Internet of things and user privacy. Results reveal that there is positive statistically significant relationship between devices for communication (r=.970), Data Transfer (r=.963), Technology regulations (r=.962), Cyber-attacks (r=.961), network for interconnections (r=.958) and user privacy. The results show that the higher the presence of devices, network connections, data transfer, Cyberattacks and application of technology regulations; the higher users need security and privacy for their data and information. These findings align with Kharagpur ideas which stated that currently there is considerable advancement of internet connection to support communication through multimedia traffic, use of telephone, music and video traffic. Internet has enabled users to access a variety of information stored at different sites (Kharagpur, 2017). Thus, Psychoula, Singh, Chen, Chen, Holzinger and Ning, (2018) argued, although privacy risks in IoT is due to data transfer and sharing information, many people have the power to decide on the offered IoT services.

Regression model Analysis findings show that any change in the device and cyberattacks (ad R Square= .951) affects the level of user privacy for using Internet of things. On the other hand, linear Regression Analysis using stepwise method was used to identify the factors that are highly affecting the privacy of respondents. Findings in table 5 show that any change in the device and cyberattacks (ad R Square= .951) affects the level of user privacy for using Internet of things. Lee and Kobsa (2017) findings supported the results of this study that the advent of the Internet of things (IoT), users are more likely to have privacy concerns since their personal information could be collected, analyzed, and utilized without notice by the networked IoT devices and services. Thus, users may want to control all such activities by explicitly expressing their privacy preferences.

Coefficients for the regression model using the stepwise method indicates how the changes in each independent variable affect the dependent variable. The findings show that independent variables; devices for communication with beta value of 0.900 indicates that for each 1 unit in this predictor there is an increase of 0.900 in user privacy. From the analysis of both predictors, 1 unit increase for the devices for communication there is an increase of 0.555 and for 1 unit increase in cyber-attacks there is an increase of 0.310 for the user concern on privacy. Although the Pearson correlation analysis indicated that all the predictors were highly and significantly correlated with the outcome, the coefficients model from regression indicates that only two predictors affects the level of need of privacy for users of Internet of things.

The results of the study correlate with what was reported In February 2016, from the USA Chamber of Commerce and the Federal Trade Commission that focused on the importance of having robust and voluntary self-regulation and security frameworks that aren't overly prescriptive. The report emphasized on designing and developing new regulations and standards for IoT and data-privacy to guide companies and device users to prevent cyber-attacks (Catherine Andrews, n.d.)

As the Internet of things (IoT) continues to gain traction and more devices connected, security becomes a major concern where businesses are increasingly being breached by attackers via vulnerable web-facing assets. In conclusion the research found that the users are not focusing much on their privacy and secure their data transmission. Participants were satisfied using IoT and connection of their devices. However, they wanted to know and understand the regulations for their security and protection of their privacy for information sharing and data transfer. Therefore, there is a need to reinforce regulations and policies to protect user's privacy on the Internet of things.

REFERENCES

Afshar, V. (2017). Cisco: Enterprises Are Leading the Internet of Things Innovation, retrieved from https://www.huffpost.com/entry/cisco-enterprises-are-leading-the-internet-of-things_b_59a41fcee4b0a62d0987b0c6

Andrews, C. El-Attrash, & Chakrabarty, S. (2016) *Your Questions Answered: The Internet of Things in Government*. Retrieved from A GovLoop Guide: https://s3.amazonaws.com/wwps-pdf/IoT-In-Government(1).pdf

Barcena, M., B., & Wueest C. (2015). The dangers of Cyber Attacks, . Retrieved from https://www.thebalancesmb.com/dangers-of-cyber-attacks-462537

Bonner, M. (2017). Dangers of cyber-attacks. Retrieved from https://www.thebalance.com/dangers-of-cyber-attacks-462537

CableLabs (2017). A Vision for Secure IoT, retrieved from https://www.cablelabs.com/insights/vision-secure-iot/#fn-30

Carlson, J., Creighton, B, Meyer, D., Montgomery, J. Reiter, A. (2014). *The Internet of Things: Security Research Study.* Retrieved from Veracode's: https://www.veracode.com/sites/default/files/Resources/Whitepapers/internet-of-things-whitepaper.pdf

Dearden, L. (2017). Russian speaking countries pose 'number one cyber threat to UK', official warn. Retrieved from http://www.independent.co.uk/news/uk/crime/russia-hacking-threat-uk-number-one-warning-cyber-attacks-wannacry-north-korea-iran-investigations-a8061521.html

Friedman, T., & Heudecker, N. (2015). Three Impacts the Internet of Things Will Have on Your Information Management Strategy, retrieved from https://www.gartner.com/en/documents/2985421

Heidt, E. (2018). Solution Path for Developing an Internet of Things Technical Strategy Retrieved from https://www.gartner.com/en/documents/3883819

Hung, M. (2018). IoT Implementation and Management — From the Edge to the Cloud: A Gartner Trend Insight Report, retrieved from https://www.gartner.com/en/documents/3873158

Karisny, L. (2015). Cyberattacks: the danger, the cost, the retaliation. retrieved from http://www.govtech.com/dc/articles/Cyber-Attacks-The-Danger-the-Cost-The-Retaliation.html

Køien, M. A. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security, 4*(65–88), 65-88.

Lee, H. & Kobsa, A. (2016). "Understanding user privacy in Internet of Things environments," *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, Reston, VA, 2016, pp. 407-412.

Lee, H., & Kobsa, A. (2017). "Privacy preference modeling and prediction in a simulated campus wide IoT environment," *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, Kona, HI, 2017, pp. 276-285.

Nguyen D. (2016). How SAP Hana Technology Could Support Your Internet of Things Strategy Retrieved from https://www.gartner.com/en/documents/3432824

Psychoula, I., Singh, D., Chen, L., Chen, F., Holzinger, A. & Ning, H. (2018) "Users' Privacy Concerns in IoT Based Applications," *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Guangzhou, 2018, pp. 1887-1894.

Rajpoot, A. K., Vashney, M. & Nailwal, A. (2016). Security and Privacy Challenges in the Internet of Things, *International Journal of Computer Science and Mobile Computing, Vol.5 Issue.6, June- 2016*, pg. 525-531

Stankovic, J. A. (2014). *Research Directions for the Internet of Things*. (IEEE) Virginia: retrieved from https://www.cs.virginia.edu/~stankovic/psfiles/IOT.pdf

Velosa, A. (2013). 'Internet of Things' Deployments Pose a Challenge to Smart-City Information Strategies, retrieved from https://www.gartner.com/en/documents/2540715

Zanella, A., Bui, N., Vangelista, L., & Zorzi, M. (2014). Internet of Things for Smart Cities. *IEEE Internet of Things Journal, 1*(1), retrieved from http://www.dei.unipd.it/~zanella/PAPER/CR_2014/IoTSmartCity2014_CR.pdf

Zlotogorski, A., Stevens, A., & Johnson, J. (2019). Starting Now, Supply Chain Leaders Should Assess the Potential for 5G Mobile Communications Networks, retrieved from https://www.gartner.com/en/documents/3913053