ACCEPTANCE OF INTERNET OF THINGS FROM SECURITY PERSPECTIVE IN MALAYSIAN GOVERNMENT AGENCY

SITI RINIY FARIZA BINTI MOHD BORHAM

UNIVERSITI TEKNOLOGI MALAYSIA

ACCEPTANCE OF INTERNET OF THINGS FROM SECURITY PERSPECTIVE IN MALAYSIAN GOVERNMENT AGENCY

SITI RINIY FARIZA BINTI MOHD BORHAM

A project report submitted in fulfillment of the
requirements for the award of the degree of
Master of Science (Information Assurance)

Advanced Informatics School
Universiti Teknologi Malaysia

JUNE 2017

To my beloved mother, Asmah bt Ismail, my late father, Allahyarham Mohd Borham bin Arif and my husband, Mohamad Faris bin Mohd Hatta who encouraged me in pursuing my master's degree

ACKNOWLEDGEMENT

Alhamdulillah, all praises are for Allah S.W.T, the Lord of the worlds, who has given me the opportunity, health, and strength to complete this research.

I would like to express my very great appreciation to Dr. Nurazean binti Maarop, my supervisor, for her guidance, patience, enthusiastic encouragement, and valuable support throughout my research journey. I have faced so many challenges during my research and her willingness to give her time so generously has been very much appreciated. May Allah S.W.T reward her for her kindness.

I also would like to extend my sincere gratitude to the main sponsor of my Master's Degree, Jabatan Perkhidmatan Awam (JPA). My grateful thanks are also extended to the expert reviewers from UTM, Dr. Muslihah Wook from Universiti Pertahanan Nasional Malaysia (UPNM) and Faizura Haneem Mohamed Ali, from Malaysian Public Sector ICT Experts for their assistance in giving suggestions and relevant review of this research. I would like to thank the selected Malaysian Government Agencies for their assistance with the collection of my data.

I would like to thank my parents for their emotional supports and their kind to me in all path that I choose. Saving the most important for last, I wish to give my heartfelt thanks to my dear husband, Mohamad Faris, whose unconditional love, patience, sacrifices, and continual support of my study over the past two years enabled me to complete this research. For my lovely children, Arissa Naureen, Aisy Nadeem and Arash Naufal, I love you more than anything. Thank you for your patience and support. Lastly, I wish to thank everybody who had helped me directly or indirectly throughout this research and it is greatly appreciated.

ABSTRACT

The internet is evolving and the next phase of the internet is known as the Internet of Things (IoT). IoT services provide new security and privacy challenges in our everyday life. The goal of the IOT is to allow things to be connected anytime, anyplace, with anything and anyone idyllically using any path/network and any service. In relation to the IoT, there are many security factors that possibly impact the effectiveness of the IoT implementation in the government. The purpose of this study is to identify the security factors that influencing user's acceptance of IoT from a security perspective to overcome the security challenges and issues and to ensure the secured IoT implementation in Malaysian government agency. Thus, a conceptual model of secure acceptance of IoT implementation is proposed. Both human and security factors are considered in the formulation of this proposed model. To understand more about the critical issues related to this study, the model of technology acceptance models such as Technology Acceptance Model (TAM) has been discussed. In this study, a TAM model was chosen with the extension of factors that will influence user acceptance of IoT technology. A quantitative method has been used as the research methodology through survey questionnaires which have been distributed via online. Data collected from 90 respondents among employees in Malaysian Government Agency. The analysis was using SmartPLS version 3.0 software. From the analysis findings, there were four (4) out of seven (7) hypothesis is significant towards the acceptance of IoT which is expected usefulness, privacy concern, perceived privacy risk, and perceived security protection. Research model predict 65.2% of the variance for behavioral intention on acceptance of IoT implementation. This study will be useful in providing understanding regarding the factors that influencing user acceptance of IoT implementation from a security perspective in Malaysian Government Agency.

ABSTRAK

Internet adalah berkembang dengan pesat dan fasa seterusnya dalam Internet dikenali sebagai “Internet of Things” (IOT). Perkhidmatan IOT dalam kehidupan seharian kita secara tidak langsung mengakibatkan kita terdedah kepada ancaman keselamatan dan privasi maklumat. Matlamat IOT adalah untuk membolehkan beberapa peralatan yang disambungkan pada bila-bila masa, di mana sahaja, dengan apa-apa dan sesiapa sahaja menggunakan mana-mana sistem rangkaian dan apa-apa jua jenis perkhidmatan. Terdapat banyak faktor keselamatan yang mungkin memberi kesan kepada keberkesanan pelaksanaan IOT di agensi kerajaan Malaysia khususnya. Tujuan kajian ini adalah untuk mengenal pasti faktor-faktor yang mempengaruhi penerimaan pengguna IOT dari perspektif keselamatan untuk mengatasi ancaman-ancaman dan isu-isu keselamatan dan memastikan pelaksanaan IOT di agensi Kerajaan Malaysia berjalan dengan lancar. Hasilnya, satu model konseptual penerimaan pelaksanaan IOT telah dicadangkan. Kedua-dua faktor sikap pengguna dan keselamatan maklumat diambil kira dalam penggubalan model konseptual ini. Untuk memahami dengan lebih lanjut mengenai isu-isu kritikal yang berkaitan dengan kajian ini, model penerimaan teknologi seperti *Technology Acceptance Model (TAM)* akan dibincangkan. Kaedah kuantitatif telah digunakan sebagai kaedah penyelidikan melalui kajian soal selidik yang telah diagihkan secara atas talian. Data dapat dikumpulkan melibatkan 90 responden di kalangan pekerja di Agensi Kerajaan Malaysia. Analisis data menggunakan perisian SmartPLS versi 3.0. Dari hasil analisis, empat (4) daripada tujuh (7) hipotesis adalah faktor penting ke arah penerimaan IOT yang kebolehgunaan, kebimbangan privasi, risiko privasi, dan perlindungan keselamatan. Model penyelidikan meramalkan 65.2% daripada varians bagi niat tingkah laku ke atas penerimaan pelaksanaan IOT. Kajian ini akan berguna dalam menyediakan pemahaman mengenai faktor-faktor yang mempengaruhi penerimaan pengguna terhadap pelaksanaan IOT dari perspektif keselamatan di Agensi Kerajaan Malaysia.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BI	-	Behavioral Intention
DoS	-	Denial of Services Attack
EEOU	-	Expected Ease of Use
EPCM	-	Extended Privacy Calculus Model
EU	-	Expected Usefulness
GPS	-	Global Position System
IoT	-	Internet of Things
LR	-	Literature Review
M2M	-	Machine-to-machine
MAMPU	-	The Malaysian Administrative Modernization and Management Planning Unit
MOSTI	-	Ministry of Science, Technology, and Innovation
NFC	-	Near Field Communication
PC	-	Privacy Concern
PLS-SEM	-	Partial Least Squares Structural Equation Modeling
PPR	-	Perceived Privacy Risk
PSA	-	Perceived Structure Assurance
PSP	-	Perceived Security Protection
RFID	-	Radio Frequency Identification Devices

SPSS	-	Statistical Package for the Social Sciences
SME	-	Subject Matter Expert
T	-	Trust
TAM	-	Technology Acceptance Model
TRA	-	Theory of Reasoned Action
TBP	-	Theory of Planned Behaviour
UTAUT	-	Unified Theory of Acceptance and Use of Technology

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Nowadays, the internet has had a substantial impact in our daily lives where space to new ideas, information, and we can communicate to the whole world. Generally, the internet is evolving and the next phase of the internet is known as the Internet of Things (IoT). The IoT, or Machine-to-Machine (M2M), is one of the main drivers for the evolution of the Internet in the direction of the Future Internet (Jara, Ladid, & Skarmeta, 2013).

The IoT refers to a collective of Internet-connected consumer devices, manufacturing systems, business tools, customer service appliances, medical equipment, agricultural sensors, and other things. The goal of the IOT is to allow things to be connected anytime, anyplace, with anything and anyone idyllically using any path/network and any service. The applications of IoT can be segmented into two (2) perspectives, which is enterprise and end users.

Today, there is a total of 1.9 billion IoT devices deployed in various end user and enterprise applications. This will grow by 2020 to as many as 23.3 billion. Of the total market, about 40 percent of all devices deployed will be enterprise devices, with the rest being in home and government (MIMOS, 2015).

In Malaysia, as mentioned in the National Internet of Things (IoT) Strategic Road Map produced by the Ministry of Science, Technology, and Innovation

(MOSTI) and MIMOS, aims to drive Malaysia into becoming a premier regional IoT hub by 2020. The technology opportunities that can be created by IoT in Malaysia are targeted in three main areas which are Economic, Social, and Governance (MIMOS, 2015).

This paradigm shift creates benefits for individuals, society, and the economy as well as raises significant challenges and security issues that needs to be addressed and considered for realizing its potential benefits (Rose Jaren, Eldridge Scott, 2015).

1.2 Problem Background

It is essential to identify the factors that influence the user acceptance of IoT. H. Evans (2015) discussed that one of the barriers to IoT successful implementation in most organizations is the perceived ease of use (Evans, 2015). Gao & Bai (2014) has also investigated the perceived ease of use and perceived usefulness that affect the IoT acceptance in China (Gao & Bai, 2014). Perceived ease of use and perceived usefulness are the significant factors that determine the user behavior intention to use the technology whereby one belief, by using IoT, will increase his/her performance (Davis, 1989).

Information security is vital with the data volume that being sent within the IoT. In relation to the IoT, there are several issues are examined to explore the challenges of the IoT technology include security; privacy; interoperability and standards; legal, regulatory, and rights; and emerging economies and development (Rose Jaren, Eldridge Scott, 2015). There are many security factors that possibly impact the effectiveness of the IoT implementation in the government.

Research that has been done by Suo *et al.* (2012), discussed that there is no technology standard about the IoT security law and regulations (Suo *et al.*, 2012). Therefore, the legislative point of view in terms of policies and regulations of the IoT are urgently needed to ensure the secure implementation. From the perspective of the user, due to lack of regulations and security concern, IoT device security may expose to the security threats by enabling unauthorized access, misuse of customer personal information, facilitating attacks on the other integrated systems which may cause individual physical harms (Dhar, 2015). Since the IoT nature which wireless and ubiquitous environment, IoT will be vulnerable to abundant malicious attacks (Gershenfeld, Krikorian, & Cohen, 2004). Hence, it is essential to implement the security features in IoT devices protocols to prevent the information leakage and vulnerability threats (Abomhara, 2014).

The privacy issue is one of the main challenges for IoT user acceptance. As for the privacy expectations, in order to respect an individual's privacy and the impartial use of their data, the data collection must be handling ethically in a secure and reliable way (Weber, 2015). In other circumstances, sometimes individual's data is potentially shared to the third parties without the user being aware of the data collections (Rose Jaren, Eldridge Scott, 2015). For example, it is becoming prevalent in user devices like smart television and video game devices. From the recent survey by Caron *et al.* (2015), data must be confidentiality, integrity, and availability (CIA). Hence, as mentioned in the recent research that has been done in Australia (2016) to protect the data transfer between sensors, and from service providers to end user, the encryption techniques should be used (Caron, Bosua, Maynard, & Ahmad, 2015).

In addition, one of the considerations in implementing IoT securely is ensuring trust in the Internet which can impact the ability of the individuals in eloquent ways (Rose Jaren, Eldridge Scott, 2015). Grau (2013) mentioned is his research that trust and governance are crucial and is an essential factor to consider when implementing IoT (Grau, 2013). In the area of new technologies like IoT, which can only develop the full potential, when the users trust and adopt these technologies. The security in IoT should be associated with a user's ability to trust their environment (Rose Jaren, Eldridge Scott, 2015). Lack of trust will make user hesitate to accept the IoT implementation. Hence, the interconnecting and interacted IoT components, which communicated to the public, must be in the trusted network to ensure a secure environment. In IoT, governance will help to strengthen the trust. Then, a security policies framework will support the interoperability and ensure the continuity of security (Grau, 2013).

As stated in the National IoT Strategic Roadmap by MOSTI and MIMOS Malaysia (2015), there is 65.8 percent of Malaysians are Internet users with 59 percent being an active user and the social media penetration in Malaysia is at 45 percent (MIMOS, 2015). With the increased numbers of the active users, security is an essential element which contributes to the technology acceptance. MAMPU (2015) has produced The Malaysian Public Sector ICT Strategic Plan (2016-2020) which stated the strategic directions of ICT implementation in Malaysian Public Sector for the next five (5) years (MAMPU, 2015). One of the actions plans is on the IoT implementation which planned to be rolled-out to all Malaysian Government Agencies by 2020 (MAMPU, 2015). With IoT implementation that has been planned by MAMPU, there will be multiple IoT devices that interconnected everywhere with various locations. It is not easy to implement IoT and it is critical for the agencies to ensure the security of IoT. If security measures are not considered in the IoT implementation, it can be misused for the malware attacks or vulnerability threats (Dr. Amirudin Wahab, 2016). Therefore, there is a need to study the various security factors that affect user's acceptance of IoT from a security perspective to overcome the security challenges and issues and to ensure the secured IoT implementation in Malaysian Government Agency.

1.3 Problem Statement

Since the IoT is the new era of computing, whereby all smart devices are communicating through the internet, the acceptance of IoT should be the major concern, especially in Malaysian Government Agencies because of the data security and privacy. The IoT implementation is vulnerable to the security risks and threats which may lead to information leakage as the data can be easily accessed by anyone and anywhere. The previous researchers mostly focused on the factors influencing acceptance on the IoT in user intentional behavior. The lack of IoT technology knowledge and security approaches of IoT due to users are unaware of the security issues, especially on the data confidentiality and trust. Hence, it remains uncertain of the security factors that may affect the acceptance of the IoT implementation securely. Thus, security measures are required for the acceptance of IoT implementation. The proposal of an evaluated model is used to study the feasibility of acceptance of the IoT from a security perspective.

1.4 Research Question

Considering the issues and problem statement mentioned, several Research Questions (RQ) of this study can be extracted and is formulated as follows:

RQ 1: What are the factors influencing the acceptance of IoT in the Malaysian Government Agency from a security perspective?

RQ 2: How to develop the acceptance model for securing IoT implementation in the Malaysian Government Agency?

RQ 3: Which factors are the most significant that determine the feasibility on acceptance of IoT implementation from a security perspective in Malaysian Government Agency?

1.5 Research Objectives

The primary objectives of this study are to examine the impact of IoT acceptance from a security perspective. In more detail, the objectives are as follows:

RO 1: To identify the factors influencing the acceptance of IoT in Malaysian Government Agency from a security perspective.

RO 2: To develop an acceptance model of IoT implementation from a security perspective in Malaysian Government Agency.

RO 3: To evaluate the proposed model and determine the feasibility of acceptance of IoT implementation from a security perspective in Malaysian Government Agency.

1.6 Scope of the Study

This research is focused on user acceptance factors of implementing IoT from a security perspective in Malaysian Government Agency. The data collection methodology will be quantitative methodology, which the questionnaire related to each theory in the model. The target audience for questionnaire in this research is an employee of the three (3) government agencies involved with IoT implementation such as MOSTI, MIMOS, and MAMPU. The survey questions will be prepared and will be sent using an online survey website. Data collected will be analyzed using SPSS software version 22.0, Microsoft Excel and/or other related statistical software.

1.7 Significance of the Study

This section will be classified into the significance of study based on both theoretical and practical contributions.

1.7.1 Theoretical Significance

In this research, theory acceptance model in technology acceptance from various researchers will be examined and analyzed. These models and approach will be reviewed and appropriate factors will be considered to propose the acceptance model to identify factors from a security perspective in IoT implementation.

1.7.2 Practical Significance

As the IoT is the new revolution of the Internet and has been widely used, this research will identify the important security factors on IoT user acceptance. This study develops an IoT Acceptance Model.

The results and recommended model will be valuable to IT managers and stakeholders of the Malaysia government agencies in feasibility analysis for the implementation of IoT and suitable security controls can be comprised of government agencies in Malaysia.

1.8 Summary

This chapter presents a brief explanation of the overall research on the feasibility study on acceptance of IoT implementation from a security perspective. This chapter contains seven sections which start with the Overview, Problem Background, Problem Statement, Research Questions, Research Objectives, Scope of the Study, and Significance of the Study. In this chapter, the factors influencing the acceptance of IoT is identified and a conceptual model will be proposed in this research to study the feasibility of acceptance of the IoT from a security perspective.

In the next chapter, the various previous research articles will be analyzed in-depth to give a strong understanding of the study and to develop the research hypothesis.

REFERENCES

Abomhara, M. (2014). Security and Privacy in the Internet of Things : Current Status and Open Issues. *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on*, 1–8.

Al-ajam, A. S., & Nor, K. (2013). Internet Banking Adoption: Integrating Technology Acceptance Model and Trust. *European Journal of Business and Management*, *5*(3), 207–215.

Al-momani, A. M., Mahmoud, M. A., & Sharifuddin, M. (2016). Modeling the adoption of internet of things services : A conceptual framework. *International Journal of Applied Research*, *2*(5), 361–367.

Amin, M. K., Azhar, A., Amin, A., & Akter, A. (2016). Applying the technology acceptance model in examining Bangladeshi consumers' behavioral intention to use mobile wallet: PLS-SEM approach. *2015 18th International Conference on Computer and Information Technology, ICCIT 2015*, 93–98.

Billure, R., Tayur, V. M., & V, M. (2015). Internet of Things - a study on the security challenges. In *Advance Computing Conference (IACC), 2015 IEEE International* (pp. 247–252).

Caron, X., Bosua, R., Maynard, S. B., & Ahmad, A. (2015). The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. *Computer Law & Security Review*, *32*(1), 1–12.

Chin, W. W. (2010). *Handbook of Partial Least Squares*.

Cohen. (1988). Statistical Power Analysis for the Behavioral Sciences. *New York*, *48*.

Davis, F. (1989). Technology acceptance model. Retrieved from https://en.wikipedia.org/wiki/Technology_acceptance_model

Dhar, V. (2015). Internet of Things and its future, 810–814.

Dr. Amirudin Wahab. (2016). Securing the Information Fabric of IoT. Retrieved from http://www.thestar.com.my/tech/tech-opinion/2016/07/14/securing-the-information-fabric-of-iot/

Elyazgi, M. G. B. (2014). Jurnal Teknologi Full paper Feasibility Study of Tablet PC Acceptance Among School Children in, *2*, 39–44.

Esa, F. S. M. (2014). *Readiness of Local Authorities in Implementing Information Security Management System (ISMS)*.

Eslami, S. G. (2010). A Survey On Factors Affecting Fuel Smart Card User Acceptance And Security.

Evans, H. I. (2015). Barriers to Successful Implementation of the Internet of Things in Marketing Strategy, *5*(9).

Fairchild, A. J., & McQuillin, S. D. (2010). Evaluating mediation and moderation effects in school psychology: A presentation of methods and review of current practice. *Journal of School Psychology*, *48*(1), 53–84.

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error, *18*(1), 39–50.

Gao, L., & Bai, X. (2014). A unified perspective on the factors influencing consumer acceptance of internet of things technology. *Asia Pacific Journal of Marketing and Logistics*, *26*(2), 211–231.

Gershenfeld, N., Krikorian, R., & Cohen, D. (2004). *The Internet of things. Scientific American* (Vol. 291).

Grau, A. (2013). Securing the Internet of Things, (September), 6.

Gupta, G., Zaidi, S. K., Udo, G., & Bagchi, K. (2015). The Influence of Theory of Planned Behavior, Technology Acceptance Model, and Information System Success Model on the Acceptance of Electronic Tax Filing System in an Emerging Economy. *The International Journal of Digital Accounting Research.*, *15*(August 2014), 155–785.

Hair, J. F. J., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2014). *Partial least squares structural equation modeling (PLS-SEM). European Business Review* (Vol. 26).

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The Use of Partial Least Squares Path Modeling in International Marketing. *International Journal of Research in Marketing*, *9*(4), 319–323.

Hossain, R., & Mahmud, I. (2016). Influence of cognitive style on mobile payment system adoption: An extended technology acceptance model. *2016 International Conference on Computer Communication and Informatics, ICCCI 2016*, 5–10.

Imtiaz, A. (2014). Feasibility Study of E-Assessment Acceptance From Teacher's Perspective.

Jara, A. J., Ladid, L., & Skarmeta, A. (2013). The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *4*(3), 97–118.

Kanuparthi, A., Karri, R., & Addepalli, S. (2013). Hardware and embedded security in the context of internet of things. *Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles - CyCAR '13*, 61–64.

Kim, C., Tao, W., Shin, N., & Kim, K. S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications*, *9*(1), 84–95.

Kowatsch, T., & Maass, W. (2012). Critical Privacy Factors of Internet of Things Services : An Empirical Investigation with Domain Experts, 200–211.

Liew, C. S., Ang, J. M., Goh, Y. T., Koh, W. K., Tan, S. Y., & Teh, R. Y. (2017). Factors Influencing Consumer Acceptance of Internet of Things Technology. In N. M. Suki (Ed.). IGI Global.

Machara, S., Chabridon, S., & Taconet, C. (2013). Trust-based context contract models for the internet of things. *Proceedings - IEEE 10th International Conference on Ubiquitous Intelligence and Computing, UIC 2013 and IEEE 10th International Conference on Autonomic and Trusted Computing, ATC 2013*, 557–562.

MAMPU. (2015). The Malaysian Public Sector ICT Strategic Plan, (August), 23.

Mcknight, D. H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site : a trust building model, *11*, 297–323.

MIMOS. (2015). National Internet of Things (IoT) Strategic Roadmap.

Othman, B. A. (2013). The Influence Of Technology Acceptance Model On Behavioral Intention To Use Internet Banking System, (December).

Park, S. Y. (2009). An Analysis of the Technology Acceptance Model in Understanding University Students’ Behavioral Intention to Use e-Learning. *Educational Technology & Society*, *12*(3), 150–162.

Perceived Usefulness, Perceived East of Use, and User Acceptance of Information Technology. (1989). *MIS Quarterly*, *13*(3), 319–340.

Preston, C. C., & Colman, A. M. (2000). Optimal number of response categories in rating scales: reliability, validity, discriminating power, and respondent preferences. *Acta Psychologica*, *104*(1), 1–15.

Rose, K., Eldridge, S., & Lyman, C. (2015). The internet of things: an overview. *Internet Society*, (October), 53.

Rose Jaren, Eldridge Scott, C. L. (2015). The internet of things: an overview - Understanding the issues and challenges of a more connected world. *The Internet Society (ISOC)*, (October).

Sadeghi, A.-R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. *Proceedings of the 52nd Annual Design Automation Conference on - DAC ’15*, *17*, 1–6.

Sheng, H. K. (2016). *Conceptual Model For Identifying Factors Affecting Trust of Software As A Service in Public Area Network*.

Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the internet of things: A review. *Proceedings - 2012 International Conference on Computer Science and*

Electronics Engineering, ICCSEE 2012, *3*, 648–651.

Terzis, V., & Economides, A. A. (2011). The acceptance and use of computer based assessment. *Computers & Education*, *56*(4), 1032–1044.

Thamadharan, K., & Maarop, N. (2015). The Acceptance of E-Assessment Considering Security Perspective : Work in Progress, *9*(3), 874–879.

Urbach, N., & Ahlemann, F. (2010). Structural equation modeling in information systems research using partial least squares. *Journal of Information Technology Theory and Application*, *11*(2), 5–40.

Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law and Security Review*, *31*(5), 618–627.

Zaremohzzabieh, Z., Abu Samah, B., Muhammad, M., Omar, S. Z., Bolong, J., Hassan, M. S., & Mohamed Shaffril, H. A. (2015). A Test of the Technology Acceptance Model for Understanding the ICT Adoption Behavior of Rural Young Entrepreneurs. *International Journal of Business and Management*, *10*(2), 158–169.

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.

Zhong, H., & Xiao, J. (2015). Apply technology acceptance model with big data analytics and unity game engine. *2015 6th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, 19–24.

Zuoan, H., Yuzhao, Z., Yusong, Y., & Hongwei, W. (2011). Consumer Acceptance of IoT Technologies in China; An Exploratory Study. *Asce*, (1), 991–996.