International Journal of Pure and Applied Mathematics
Volume 118 No. 24 2018
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

Research on risk endurance influence to Use behavior of Internet of things -Focus on personal privacy information and safety-

CHENXI HU and Kyeong-Rak Lee[1], Sang-Joon Lee[2*]
[1]Free21+ e-Service Team,
Chonnam National University, 61186, Korea
hcx12pride@hotmail.com and kryi@nate.com
[2]School of Business Administration,
Chonnam National University, 61186, Korea
s-lee@chonnam.ac.kr

Abstract

Background: In recent years, the development of Internet of Things (IOT) has attracted the interest from business community and academic areas. IOT is considered as the next opportunity of the trillion marketing. The styles of production and normal life, as well as the capacity in information acquisition have changed a lot by the emergence of IOT. Meanwhile adumbrate a worldwide revolution in information technique.

Methods: The core concept of IOT is perception, control, transmission and intelligence. With the spread studies of IOT technology and its applications, information can be reliably transmitted, intelligently process and collect, storage, transmitted and applied. So around these situations, this dissertation tries to study the problem of using personal privacy information in IOT. Therefore, the new security and privacy problems will arise. The purpose of this paper was to examine IoT Use Behavior related with Risk Endurance

which is affected by Perceived Importance of Privacy, Perceived Importance of Safety, Perceived Intention to Sacrifice Privacy, Perceived Intention to Sacrifice Safety. In this paper we proposed research model and hypothesis, and collected data by collecting questionnaire, and did frequency analysis, descriptive statistics analysis, reliability analysis, factor analysis and regression analysis by SPSS.

Findings: First, based on lots of representative literatures, the history and evolution of IOT, The key technologies and typical applications of IOT. And then summarizes the features, expressions and protection of personal privacy information. At the same, analyze the essential aspects of personal privacy information. Second, analysis several privacy protection measures of IOT, such as legally enforcement, ethic self-discipline and advanced technologies. Label destruction, machine mode and user model are summarized further from technical analysis. The empirical analysis model is constructed by the combination of decision tree. Data are collected by scenario training and questionnaires for different privacy protection modes. Finally, on the basis of information economics theory, the risk endurance is quantized and mathematical to capture the influence from different personal privacy parts on consumer's IOT use behavior.

Improvements: IOT is the form integration of the latest of the information technology network, its core idea is comprehensive perception and reliable courier and intelligent control, networking personal privacy information is unique form of expression has become one of the main important factors that influence IOT, and from research result for IOT using behavior, consumer's intention of endurance of risk is strong. So focus on this problem and to make it transparent to customers will very helpful to entrepreneur or government to pursuing this technology.

Key Words : Internet of Things, Risk Endurance, Use Behavior, Privacy, Information.

1 Introduction

At present, many countries in the world already had Internet Of Things (IOT) into the strategic industry revitalization plan, such as the United States of America's "smart earth", the EU's "Internet of things" plan, Japan's "IJPN plan" and so on . These plans are known as the next one trillion market opportunity, its importance and development potential has no doubt.

On the Internet of things, Dimitris, a Swiss scholar, gives a description of the Internet of things, which is based on the Internet, extending and expanding the user's client to any kind of networks form the information exchange and communication between any articles (M2M)[1]. In Popular the sensor is embedded and installed into the grid, dams, bridges, railways, oil and gas pipelines and other natural objects, the construction of intelligent information infrastructure, and in all kinds of wireless sensor networks based on cloud computing technology background data processing power support, and the existing Internet integration, the implementation of real-time management and control of personnel, machinery and equipment, to more sophisticated and collaborative management of production and life, improve resource utilization and productivity levels[2].

In the daily life people will feel like the earth shaking changes, and things can "speak": the expired food in the refrigerator to remind you to deal with, clothes tell you whether and the water temperature is appropriate, shopping malls do not have to wait in line. The Internet of things is a new type of virtual network and real world real time interactive system, which is characterized by the ubiquitous data perception, information transmission and intelligent information processing based on wireless communication. But at the same time, such a system can also convenient to collect information on the daily life of the individual a lot, so as to become ubiquitous in our lives monitor, that is, the Internet of things has brought a new privacy disclosure risk: real-time and accurate location information, personal time and space is been tracked, historical information is been stored, behavior habits were excavated. Therefore, the promotion and application of the Internet of things technology, on the one hand, will significantly improve the economic and social efficiency, on the other hand, the state and enterprises,

citizens of information security and privacy issues raised a serious challenge.

One of the core technologies of the Internet of things is RFID Frequency Identifications (Radio) technology, and one of the problems in the application of RFID technology is privacy issues. Research practice, the RFID tags placed on the goods, business organization will be able to get personal information about the shopper, which will likely result in the leakage of personal privacy[3]. Due to the high degree of the Internet of things technology, and other information technology adoption, privacy protection of the Internet of things technology adoption behavior constitutes a greater impact, Ohkubo et al research shows that two privacy issues make RFID technology adoption more complicated: the personal information of consumers and consumers' physical location tracking. He also believes that due to the different degree of tolerance of privacy disclosure has resulted in the difference of the perceived importance of the above two privacy issues. Hossain and Probutok extended the technology acceptance model (TAM) to join the perceived privacy, perceived security and other factors, through the investigation of 307 students to learn the RFID technology to explore the impact of consumer adoption of RFID; they found that convenience, culture, and perceived privacy are the main factors affecting consumer RFID technology[4]. Information transparency and information sharing is the biggest feature of the Internet of things, information collection is ubiquitous and pervasive, and all kinds of information is easy to be copied, transmitted and integrated, which can provide personalized service and improve customer satisfaction[5]. However, if do not to take appropriate protective measures, these information on personal privacy will cause serious threat. From this sense, consumers, managers and researchers should see personal information is a double-edged sword, in the safety protection used carefully, it can increase the participant's utility, if arbitrary abuse will the participants bring harm. In this paper, we find the importance of personal privacy information in the research of the Internet of things technology, and explore the relationship between them.

2 Literature Review

The Internet of things is a comprehensive information system, which is realized by perceiving the physical world. "Perceived world, service human" is the core concept of the Internet of things. The information is the key element of the Internet of things. We can experience the real service provided by the Internet of things from the following two examples.

2.1 IOT situations over the world

The Internet of things technology in the logistics supply chain is also widely used in the field. 2001's casual fashion giant GAP, Inc., the company used RFID to track the management of apparel, obtained 99.9% of the inventory accuracy and increased its sales revenue increased by 2 to 7 % [6]. Retailers giant WAL-MART has used RFID technology in its logistics warehouse in 2003, and has asked its top 100 major suppliers to use electronic tags before 2005[7]. Now with the rapid development of e-commerce, the third party logistics enterprises have generally through the Internet WEB services to provide consumers with the flow of goods purchased goods tracking, all of these, the Internet of things technology into business activities also provide us with a convenient life.

Therefore, under the background of the Internet of things technology, a wide variety of data acquisition and sensing devices are ubiquitous, sensing and transmitting real-time status information of people's activities and environment. This kind of transparent access can provide personalized services, however, the user's personal information (such as body, location, current activity content, and even consumer preference) is collected, stored and processed without any sense of the user. Therefore, the pan in the Internet of things, the application of the Internet of things has become a double-edged sword, the domestic and foreign experts and scholars have made great attention to the application of the Internet of things can not only bring us convenience but also will lead to a series of ethical issues. In particular, the acquisition, storage, conversion and use of personal privacy constitute a significant challenge to the right of privacy of individuals[8]. Concerns about privacy and security concerns have become an important obstacle to the de-

ployment and application of things, as early as 2003, the United States government to try to embed the RFID chip in the passport, but due to privacy infringement and delay until 2008 after the implementation[9].

2.2 The establishment of the concept of personal privacy information

In this paper, the privacy of the individual social activities with the inclusion of the time, space, process and other environmental information of the polymer, different cultural background determines the different privacy is different, individual personality characteristics of the understanding of privacy is not the same, but also closely related to the situation of the scene, the privacy demands are not the same. Privacy is not entirely the objective existence of, but very subjective a cognitive process, each people have independent privacy boundaries and privacy threshold, need in-depth communication to clear.

2.3 Personal privacy information and perceived privacy

Nowak and other studies suggest that consumers express a great concern for the personal information (such as name, age, address, shopping preference, etc.) that can be traced back to the consumer's history, so they will be influenced by the degree of perceived privacy in consumer decisions[10]. Moreover, they put forward the influence factor model of the importance of consumer perceived privacy, and analyze the factors such as the information gathering and the perception information control. Dinev and other through the study of e-commerce B2C consumer online shopping behavior, pointed out that consumers in the online shopping process of voluntary or non-voluntary disclosure of personal information, and then have a fear of the consequences of its disclosure, causing privacy concerns[11].

2.4 New progress in research on personal privacy issues

Mcgrath think of others by monitoring or surveillance is actually has existed for a long time, at least this is personal privacy protection than earlier[12]. However, the history of the privacy issues of concern has never been so much attention, for fear of their own private life by the invasion and anxiety, in order to avoid their privacy exposure to fight; people deeply felt that modern information technology means to provide a violation of privacy has not had the convenience.

Close the door, thick clothes, the mouth has been difficult to prevent the closure of personal privacy information is acquired. Objectively and subjectively, I struggle in the whirlpool of contradictions, and I can get the privacy of others, and the objective of the personal privacy of the public and the pain. Surveillance in public to promote social harmony and security, for the benefit of humanity's personal data (such as gene mapping) collection should be supported, personal privacy information can not completely give up, and information disclosure and compelling, how to choose is worth thinking problem? Appropriate personal privacy protection, the solution of the appropriate public and private boundary problem is the basic point of this article.

2.5 Features of privacy information in the Internet of things

2.5.1 High-Sensitivity

Information and data flow of the Internet of things, mainly from the people living closely related to the environment, events, objects, such as personal information, the location of the real-time position, carrying the object and personal activities, living habits and shopping preferences, etc.. This information is a lot of personal information is sensitive, people certainly do not want their whereabouts are tracked at any time, personal identity information is malicious access. In addition to sensitive information itself, access to these information is also much easier than it is today's network form, and even in the case of other people can easily get the information.

2.5.2 Truth

Information in the Internet of things is from the collection object itself, is the real state of the reflection, such a hand data is very difficult to counterfeit, and the structure of the network of the system logic is very strong, the network of individual data is accurate and reliable, to achieve data sharing and effective control. It can be said that the real and reliable data is the basic requirements of the Internet of things.

2.5.3 Systemic

The data in the Internet of things has a strong logical connection. The data information of the user may be distributed in many different databases and applications. With the expansion of the scope of the user's activities, information is also spread. In addition, there is a link between the same information of different individuals, in order to adapt to the intelligent data processing in the Internet of things, to complete the natural, social, human and orderly harmony.

3 Research framework and Hypotheses

This research domain to study on risk endurance influence to use behavior of IOT, research methods mainly through three ways: descriptive statistics, exploratory research and confirmatory analysis. The descriptive statistics is to classify and summarize the collected data, calculate mean, variance, and so on. It is found and summarized the behavior characteristics of the studied objects, such as concentration, dispersion, distribution and so on. Exploratory research mainly from the data to find the correlation between the various variables, this correlation is not known in advance or just a guess, through exploratory research to verify, such as principal component analysis, clustering, etc. The verification of the study is to prove the relationship between the variables, and establish a set of hypotheses, and then test the hypothesis by using statistical data. In this paper, the three methods of analysis will be based on the purpose of the study.

3.1 Research model

From literature research we use risk endurance theory to build the research model, like if consumer would sacrifice a little of their privacy and safety to get new experience more convenience and benefit from IOT. Perceived importance of privacy constitute that consumer see their privacy level for now more important or sacrifice some and trust in new technology because it is giving a totally new experience and convenience as shown in figure 1.

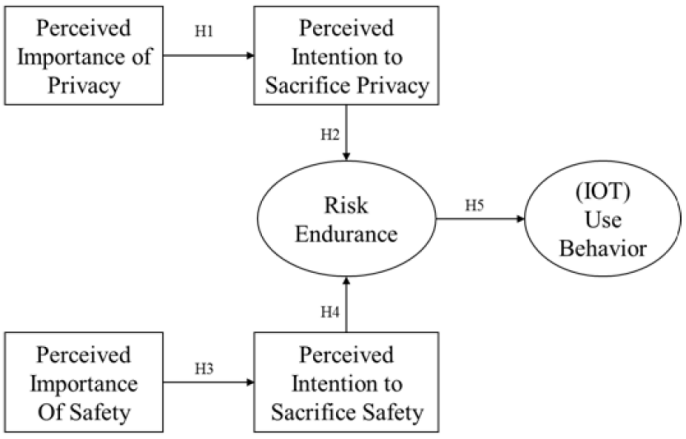

Figure 1: Research Model

3.2 Hypotheses

[H1] Perceived Importance of Privacy do negative influence to Perceived Intention to Sacrifice Privacy.

[H2] Perceived Intention to Sacrifice Privacy do positive influence to Risk Endurance

Things will give consumers more privacy information disclosure, consumer awareness of privacy concerns will increase; the degree of trust in the Internet of things will be reduced. On the other hand, the degree of attention to personal privacy information is influenced by the degree of personal privacy, the more sensitive to personal privacy; the more important is the change of personal privacy. The greater willingness to sacrifice thus the higher endurance of the risk.

[H3] Perceived Importance of Safety do negative influence to Perceived Intention to Sacrifice Safety.

[H4] Perceived Intention to Sacrifice Safety do positive influence to Risk Endurance.

Knowledge security is the information system in the transmission and storage, consumers believe that their personal information will not be inappropriate to the third party in a certain way to browse, transfer and use, bringing with them the possibility of not consistent. Perceived safety and perceived privacy are similar, but also a subjective concept, but they are based on objective reality. Perceived security is the security of personal information in the process of transmission and storage, which is objective, but because of the influence of personal experience, risk attitude and personality, it is not the same for different consumers[13]. Thus, perceived security is the product of the combination of objective safety and consumer's subjective feelings and expectations.

[H5] Risk Endurance do positive influence to IOT Use Behavior.

Things technology services will be very common, such as mobile payment requires banks, operators, consumer participation in any link to provide services may involve privacy issues and security issues, therefore, consumers will be affected by the risk of Internet service providers will affect the willingness to take the risk of Internet service providers, and the willingness to adopt the Internet of things.

4 Methods

4.1 Questionnaire design, data collection and analysis method

Scale design and data analysis

In this paper, we use the method of social investigation, which is a kind of method to collect data and analyze the data. According to the survey, the questionnaire was chosen to set the variable, and each variable was designed to measure the problem.

4.2 Data control statistics

Table 1: Initial Set of features used for the experimentation

Data control statistics							
Gender	%	Age	%	Occupation	%	Education	%
Male	62.9	≤20	1.5	Civil servant	3	≤ High School	1.3
Female	37.1	21-30	52.3	Professional and technical occupation	7.5	Junior College	18.3
		31-40	18.4	Management	9.0	Undergraduate	50.0
		41-50	19.2	General staff	28.6	Master	26.6
		51-60	7.5	Free professionals	1.1	Ph.D.	3.8
		≥60	2.3	Students	48.1		
				Non job	2.6		

From table1 we can find out that age, education and occupation of objective is in the normal level, so the investigation results can be trusted.

5 Results

5.1 Reliability and validity analysis

As shown in table 2, the internal consistency reliability of the questionnaire's reliability and the internal consistency reliability of the questionnaire, which was reflected by the intrinsic relationship between the amount of the questionnaire, and the essence of the test questions whether the measurement of the same content or characteristics.

Table 2: Reliability and validity Analysis

Hypothesis	Questions.	Factor load	SE	AVE	Cronbach's α
PIOP	Questions No.1a	.693	0.00	0.690	0.713
	Questions No.1b	.593	0.131		
	Questions No.1c	.885	0.130		
	Questions No.1d	.854	0.152		
PISP	Questions No.2a	.825	0.00	0.751	0.779
	Questions No.2b	.736	0.099		
	Questions No.2c	.929	0.089		
	Questions No.2d	.879	0.130		
PIOS	Questions No.3a	.890	0.00	0.763	0.796
	Questions No.3b	.887	0.102		
	Questions No.3c	.902	0.099		
	Questions No.3d	.822	0.167		
	Questions No.4a	.943	0.00		

PISS	Questions No.4b	.918	0.089	0.805	0.842
	Questions No.4c	.903	0.100		
RE	Questions No.5a	.485	0.00	0.775	0.868
	Questions No.5b	.730	0.159		
	Questions No.5c	.835	0.097		
UB	Questions No.6a	.708	0.00	0.747	0.805
	Questions No.6b	.765	0.181		
	Questions No.6c	.672	0.174		

5.2 The test results of path parameter

As can be seen from the table 3, all the hypotheses are supported. In addition, in addition to risk tolerance factors, the rest of the statistical significance of the standard path coefficient of the absolute values are greater than 0.2, which is the corresponding hypothesis.

Table 3: the test results of path parameter model

Path	Coefficient	S.E	P	Hypothesis	verification
UB<-RE	0.358	0.059	**	H5	verification
PISP<-PIOP	-0.347	0.110	***	H1	verification
PISS<-PIOS	-0.239	0.099	***	H3	verification
RE<-PISP	0.243	0.048	**	H2	verification
RE<-PISS	0.900	0.053	***	H4	verification

P=*** means P<0.01, ** means P<0.01, * means P<0.05

5.3 Verification of conditioning effects

In this research, the measurement variables of performance expectation, effort expectation and social influence are standardized, then the product of the empirical of the Internet of things, and then the new latent variable, and then get the original model and adjustment mode, see from figure 2.

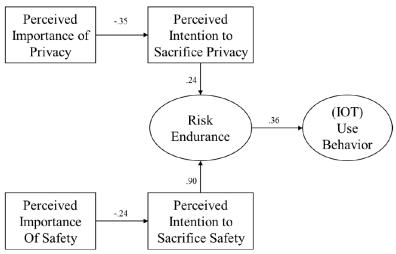

Figure 2: Model data validation result

6 Conclusion

The research shows that the security of the Internet of things and the privacy of individual privacy constitute the important factors of the user's perceived risk, and have a direct impact on the user's adoption intention. The empirical analysis of data collected by this research is basic and reasonable, and the interpretation of user acceptance intention is acceptable, and the model can reflect the main influence factors in the application of Internet of things technology. H5 has been supported, consumer perceived risk tolerance is positively affecting the adoption of Internet services, and that is, consumers can bear a greater risk, for example, willing to sacrifice more security and to give up more privacy information, then, more willing to accept the Internet service.

The research shows that the security of the Internet of things and the privacy of individual privacy constitute the important factors of the user's perceived risk, and have a direct impact on the user's adoption to IOT. The empirical analysis of data collected by this research is basic and reasonable, and the interpretation of user acceptance intention is acceptable, and the model can reflect the main influence factors in the application of Internet of things technology. Risk endurance also be used in psychology discipline, but when development brings innovation the consumer's psychology is very important for promoting new technologies, new business ways and new changes.

IOT is the form integration of the latest of the information technology network, its core idea is comprehensive perception and reliable courier and intelligent control, networking personal privacy information is unique form of expression has become one of the main important factors that influence IOT, and from research result for IOT using behavior, consumer's intention of endurance of risk is strong. So focus on this problem and to make it transparent to customers will very helpful to entrepreneur or government to pursuing this technology.

References

[1] Dinev T, Hart P, *Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact,* International

Journal of Electronic Commerce, 2005, 10(2), pp .7-29.

[2] Dimitris K, *Closed-Loop PLM for Intelligent Products in the era of the Internet of Things,* Computer-Aided Design, 2011, 43(5), pp. 479-501.

[3] Mark W, *Some Computer Science Issues in Ubiquitous Computing,* Communications of the ACM, 1993, 36(7), pp. 7584.

[4] Ohkubo M, Suzuki K, Kinoshita S, *RFID Privacy Issues and Technical Challenges,* Communications of the ACM, 2005, 48(9), pp. 6671.

[5] Hossain M M, Prybutok V R, Consumer Acceptance of RFID Technology: *An Exploratory Study,* IEEE Transactions on Engineering Management, 2008, 55(2), pp. 316-326.

[6] Naresh K M, Sung S K, Tames A, Internet User's Information Privacy Concerns(IUIPC):*The Construct,* the Scale and a Causal Model, Information System Research, 2004, 15(4), pp. 336-355.

[7] Ardagna C A, Cremonini M, Damiani E, Vimercati S D, Samarati P, *Location Privacy Protection Through Obfuscation-Based Techniques,* Lecture Notes in Computer Science, 2007,4602, pp. 47-60.

[8] Anthony D, Henderson T, Kotz D, *Privacy in Location-Aware Computing Environments,* IEEE Pervasive Computing, 2007, 6(4), pp. 64-72.

[9] Abell P, Item tracking: *myths and realities,* RFID Journal, 2003, 12(2), pp. 219-232.

[10] Romanow K, Lundstrom S, RFID in 2005: *The What is More Important Than the When with Wal-Mart Edict,* AMR Research, 2003, 8(2), pp. 9-22.

[11] Christoph P M, *Security and Privacy Challenges in the Internet of Things,* Electronic Communications of the EASST, 2009, 17, pp. 1-12.

[12] Weber R H, *Internet of Things-New Security and Privacy Challenges,* Computer Law & Security Review, 2010, 26(1), pp. 23-30.

[13] Nowak G J, Phelps J E, Understanding Privacy Concerns: *An Assessment of Consumers' Information-related Knowledge and Beliefs,* Journal of Direct Marketing, 1992, 6(4), pp. 28-39.