Indian Journal of Science and Technology, Vol 9(44), DOI: 10.17485/ijst/2016/v9i44/105106, November 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A study on Psychological Conflict Elements Affecting Intention to Use Biometric-Based Non Face-to-Face Authentication System in Financial Transactions

Choong-Keun Han[1], Jung-Wan Hong[2] and Yen-Yoo You[1]*

[1]Department of Knowledge Service and Consulting, Hansung University, Republic of Korea; ckhan1009@gmail.com, threey0818@hansung.ac.kr
[2]Department of Industrial and Management Engineering, Hansung University, Republic of Korea; jwhong@hansung.ac.kr

Abstract

Objectives: This research tries to discern psychological conflict elements related with biometric-based non face-to-face authentication system in financial transactions, and examine how these elements affect the intention to use the biometric system. **Methods/Statistical Analysis**: Research data were collected from the survey to users. To test goodness of fit of the research model and hypotheses, structural equation modeling was used. **Findings**: The analysis found out that perceived risk characteristics like privacy concern and routine seeking personality have significant effects on usage conflict, and, then, usage conflict has negative effect on the intention to use the biometric system. **Improvements/Applications**: This research implicates that financial institutions should be aware of antecedent variables affecting usage conflict and try to make efforts to reduce such negative perception on the biometric system.

Keywords: Biometrics, Information Privacy Risk, Negative Mass Media, Privacy Concern, Routine Seeking Personality, Usage Conflict

1. Introduction

Recently, with the expansion of importance of non face-to-face channels, enlargement of the market of Fintech which combines finance and IT, abolition of obligatory use of 'authentication certificate' to activate Fintech, launching of 'Korean-type Internet-specific bank', and strengthening of the Personal Information Protection Law, the financial industry faces a paradigmatic change[1,2]. And, with the trend of strengthening security, biometric technology is in the spotlight again. When one pays with smart phone and use internet banking, non face-to-face authentication and privacy protection become important.

Most existing researches on biometric technology deal with security matters including biometric information protection technology or software technological R&D and others. In particular, there are not sufficient researches

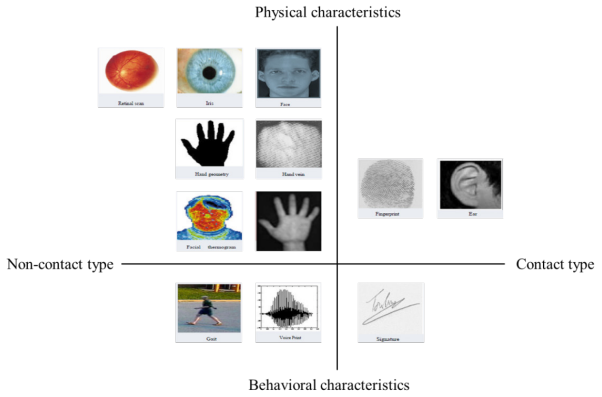

Figure 1. Classification of biometric authentication methods Source: Oh D Y [8], revised by the authors of this paper.

*Author for correspondence

on biometric technology use as authentication method in financial transactions from the perspective of users. Thus, this research tried to empirically examine psychological conflict elements in using the biometric system in non face-to-face financial transaction users.

Now, financial institutions try to expand use of system infrastructure on financial transactions (smart phone simplified settlement, digital kiosk, and ATM, etc.). In this situation, if there are some negative variables in the intention of end users in using biometric system, it will have connotation for financial institutions to adopt biometric technology in non face-to-face authentication.

2. Theoretical Background

2.1 Biometric Technology

Biometric technology is defined as "the method of examining or perceiving physical or behavioral characteristics of specific living persons"[3-5].It is the technology of using unique characteristics of individuals as measurement units for authenticating them, based on physiological and behavioral characteristics of human beings, and of using biological characteristics in authentication through automated apparatuses. Biometric technology is used as the means of identifying individuals by extracting bio information (fingerprint, iris, vein, face, voice, and hand shape, etc.) of each individual, registering the information in the storage device of the biometric system, and, then, measuring the characteristics of biometric information of an individual through biometric entry device, matching and comparing the characteristics with registered information, and determining the compatibility of them[6].

Biometric technology uses physical characteristics such as fingerprint, hand shape, face, iris, retina, and vein, etc. or behavioral characteristics like signature, voice, and gait, etc.[7] as shown in Figure 1. It can be divided into contact type and non-contact type[8]. It can be widely applied in various industries. The cases of using biometric technology per area are summarized in Table 1[9].

2.2 Characteristics of Perceived Risks

This research intends to examine previous researches dealing with characteristics of perceived risks such as information privacy risk, privacy concern, and negative mass media.

Table 1. Use of Biometric Technology

Area	Examples of using the technology
Finance	E-commerce/ATM authentication Payment
Security	Authentication for entering and exiting facilities Authentication for user of mobile phone, notebook, or car, etc.
Airport	Immigration control Quarantine (tele-measurement of body temperature)
Defense/ Investigation	Unmanned monitoring and search/rescue Voice analysis and detecting criminal
School	Identification of examinees Meal plan, book check-out
Public	Electronic voting system Identification card Unmanned document issuing machine
Medical field	Remote medical care Issue of unmanned prescription
Marketing	Estimation of age/gender of visitors by facial identification Point accumulation by finger identification

2.2.1 Information Privacy Risk

In the aspect of privacy risk, the biometrics area is located at the center of various discussions among all the areas. It means that biometrics is more vulnerable to privacy risk than the case of other areas. At the beginning, financial institutions, being hurried of rapid growth, did not well prepared with privacy protection of users, and a variety of cases of privacy violation occurred. With the increase of such cases, many kinds of privacy risk users did not aware of have been known. The degree to which users perceive risk affects their decision-making. Thus, it is important whether users directly perceive privacy risk. That is, even if something is very risky in the aspect of privacy, if users do not recognize the risk, it does not affect their behavior[10]. This research viewed that the perception of biometrics user serves as an element forming resistance in his or her use of biometrics.

2.2.2 Privacy Concern

Information privacy concern is defined as the concern about the possibility of losing privacy caused by voluntary or involuntary exposure of information[11]. This is a con-

cept different from perceived risk. It is perception of the risk of privacy being violated which can occur in Internet environment. Privacy concern is the worry that his or her personal privacy can be violated[12].

Privacy concern is internal condition of each user, and is expressed differently depending on personality of user and level of service provided to user. If a user wants more personified service, the user tends to provide more personal information, even if the user has privacy concern. Considering such things, privacy concern of user is dependent on situation, and there are conflicting elements in the decision-making process[13]. It means that even if there is perception of privacy risk, it does not necessarily mean concern about privacy violation, and unlike perceived risk, it can be controlled by various protection apparatuses.

2.2.3 Negative Mass Media

Mass media communication is the means in which one or a small number of massage senders can deliver message to a large number of receivers by mobilizing mass media such as radio, television, newspaper, and magazine, etc.[14].

In the theory of diffusion of innovations,[15] said that communication using mass media channels as well as man-to-man channels has considerable explanatory power in understanding the diffusion process of innovations. And, he suggested the following generalization that, in the innovation decision process, mass media is relatively more important in knowledge stage, and man-to-man channel is relatively more important in persuasion stage, and that, to early adopters who adopt innovations before diffusion starts in full scale, mass media is relatively more influential than man-to-man channel.

As described before, to understand psychological resistance to use of biometric technology, it can give new connotation to examine the effect of mass media.

2.3 Routine Seeking Personality

Routine seeking personality is tendency of refusing changes and hating giving up old things[16,17]. Various organization theorists view 'resistance to giving up previous habits' as general characteristics of resistance[17]. Some researchers argued that the reason why consumers who favor seeking routines refuse changes lies in the fact that familiarity creates comfort[16]. That is, when a new stimulus is given, familiar response is not proper to the situation. So, the person gets stress from it. Consequently, routine seeking tendency accompanies preference of work, procedure, and environment, etc. which are customized, traditional, and easily predictable[18].

Consequently, consumers high in tendency of seeking routine are expected to refuse something they should give up familiar customs because of innovation and resist changes.

2.4 Usage Conflict

Dissonant relationship is psychological conflict generated when someone perceives that cognitive elements on the same object are not mutually harmonized, and it works as motive to change one's attitude or behavior on the object. That is, as dissonance causes psychologically very unpleasant tension, dissonance leads one to make efforts to change either of the incompatible cognitions[19].

In[20] argued that, to lower the occurrence of cognitive dissonance of customers, it is necessary to adopt the strategy to reduce risk cognition, and that, to maintain consistent cognitive state or to get harmonious cognitive state, customers reduce cognitive dissonance by rationalizing to reduce dissonance.

As such, cognitive dissonance theory is the theory explaining link between attitude and action through the relationship between cognitive elements. This research will use the concept of cognitive dissonance by conceptualizing it as a term called 'use conflict'.

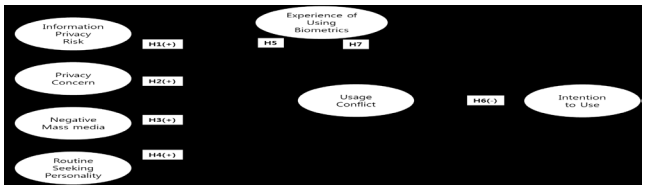

Figure 2. Research model.

2.5 Intention to Use

To measure whether a new innovative information technology or system will succeed or not, one usually uses 'user satisfaction' or 'intention to use the system', and 'intention to use the system' is the will of the user to use the system, and decision of the user toward target behavior[21]. Consequently, 'intention to use the system' has been studied a lot as the criteria of success on acceptance and realization of the information system[22]. In[23] and[24] defined intension to use as strength of intention to use information system. And, previous researches suggested that, as intention to use functions as an important element to

decide real activity, if we grasp intention to use, we can predict real activity[25].

3. Research Model and Hypotheses

3.1 Research Model

The aim of this research is empirically examine how perceived risk characteristics and routine seeking personality, which is personal trait of the user, have effect on use conflict, and how usage conflict has effect on intention to use in the use of authentication system in financial transactions. And, as experiences of using general biometric media are closely related with intention to use biometric system, this research will use 'Experience of Using Biometrics' as moderating variable, and test the effect of the moderating variable.

Accordingly, this research, based on existing theoretical basis and previous researches, constructed the research model shown in Figure 2.

Theory of Planned Behavior (by the relationship between) is the basis of the research model of this research. That is, the relationship between Usage Conflict and Intention to Use is proven by the relationship between attitude and intention to act, and the relationship between perceived risk characteristics and routine seeking personality, on the one hand, and Usage Conflict, on the other hand, is proven by the relationship between behavior belief and attitude in TPB.

3.2 Research Hypotheses

3.2.1 The Relationship between Perceived Risk Characteristics + Routine Seeking Personality and Usage Conflict

With the recent change of information technology environment, information privacy risk emerges as one of the most important elements. In particular, biometric technology area has become the issue of various debates more than any other areas in the perspective of privacy risk.

This research defines information privacy risk as 'the degree of risk perception on the possibility of losing control following the provision of biometric information'.

According to[26], the same information privacy risk can vary in risk types and degrees depending on users. In[27] argued that the more a company collects and keeps personal information of customers, the more frequently personal information like unique information of customers the company uses, the higher the likelihood of the company violating privacy of customers.

According to[10], as the degree to which the user perceives something as risky affects the decision-making of the person, it is the most important whether the user directly perceives information privacy risk. That is, even if there is real risk, if the user does not perceive it as risky, such a risk does not affect the behavior of the user.

Thus, based on the above theoretical discussions and previous researches on information privacy risk, this research sets the following hypothesis.

H1: Perceived information privacy risk following the provision of biometric information will have positive (+) effect on usage conflict.

In[11] defined privacy concern as the concern on the possibility of losing privacy as the result of information being exposed voluntarily or involuntarily. It is a concept different from perceived risk. Privacy concern is worry on the possibility that one's own privacy can be violated [28,12]. This research defined privacy concern as 'the concern on the possibility of personal bio information being leaked which can happen when someone uses the biometric system.

In[29] found that in e-commerce, the higher privacy concern of customers get, the lower their intention to use it. But,[30] proved that even those who are high in privacy concern can be relatively active in revealing personal information if they are high in self-efficacy[31].

Consequently, this research views privacy concern as antecedent element which can cause usage conflict in providing bio information and using biometric technology, and, based on the above theoretical discussions and previous researches, sets the following hypothesis.

H2: Privacy concern following provision of bio information will have positive (+) effect on usage conflict.

In[15] said that to understand diffusion of innovations and resistance to them, communication through mass media is important. As mass media, with the characteristics of generality, popularity, and public character, leads to low psychological defense and high acceptance[32].

On the other hand[33], based on impression formation theory, argued that people tend to give weight to negative message rather than to positive one, and focus more on the negative one.In[34] explain negativity effect in which one intends to receive negative message more seriously.

And[19] said that because of the effect of mass media which highlight negative aspects of SNS, SNS usage conflict can occur.

This research defines Negative Mass media as 'the degree to which one perceives biometric technology-related negative message through mass media'. Considering negative message delivered by mass media as antecedent element which can cause conflict in usage of biometric system, based on the above theoretical discussions and previous researches, this research sets the following hypothesis.

H3: Negative information delivered from mass media will have positive (+) effect on usage conflict.

In[16] and[17] defined routine seeking personality as the tendency of hating giving up old habits against changes. This research defined it as 'the degree to which one is reluctant to be changed like reluctance to abandoning habits'.

In[35] argued that members high in routine seeking personality tend to favor the work they have done up to now and staying in comfortable conditions, and that members who are strict and close-minded are not high in their tendency to enjoy new situation or try to adjust themselves to the situation[36].

In[18], in their study on personal characteristics and psychological resistance to organizational changes, found out that the higher routine seeking personality gets, the higher psychological resistance becomes, which means that the more one sees changes negatively and like the existing ones, the higher his or her psychological resistance to changes.

Based on the above theoretical basis and previous researches, this research sets the following hypothesis.

H4: The higher routine seeking personality is, the higher usage conflict becomes.

H5: The relationship between perceived risk characteristics + routine seeking personality and usage conflict can vary depending on the experiences of using biometric media.

3.2.2 The Relationship between Usage Conflict and Intention to Use

Cognitive dissonance suggested by[37] is cognitive unequilibrium which appears when one has contradictory cognitive elements. Cognitive dissonance theory classifies the relationship among cognitive elements into three types: harmonious relationship where those elements are consistent; non-relationship where they are unrelated; dissonant relationship where they contradict one another. In particular, dissonant relationship is psychological conflict which occurs when one perceives that cognitive elements to the same object are not harmonious, and it motivates one to change one's attitude or behavior. This research defines usage conflict as 'the degree to which one feels psychological discomfort and conflict in using biometrics.

Table 2. Operational definitions of variables and the number of measurement items

Variable	Operational definition	No of questions	Related researches
Information Privacy Risk	The degree of risk perception on possibility of losing control following provision of bio information	5	29 11
Privacy Concern	The degree of concern on possibility of bio information being leaked which can occur when one uses biometric system	4	12 41 11
Negative Mass Media	The degree of perceiving biometric technology-related negative message through mass media	4	15 42
Routine Seeking Personality	The degree of reluctance to accept change, like hating abandoning habits	3	18 35
Usage Conflict	The degree of discomfort and conflict in using biometric system	6	37 19
Intention to Use	The degree of intention, plan, or possibility to use biometric system	4	24 23
Experience of Using Biometrics	Experience of having used general biometric media	1	24

In[37] said that if dissonance takes place, one loses consistency in attitudes and behavior, and it works as motive to dissolve the dissonance.

In[38] empirically showed that after procuring digital convergence products, customers, due to cognitive dissonance, avoid buying those products. In[39,40] report that psychological disharmony which means conflict condition has considerable effect on terminating to use SNS.

Considering such research results, it is expected that the user who is in psychological disharmony, that is, usage conflict because of perceived risk characteristics on biometric system and routine seeking personality will not intend to use it or avoid using it.

Consequently, based on the above theoretical discussions and previous researches, this research sets the following hypotheses.

H6: Biometric system usage conflict will have negative (-) effect on intention to use.

H7: The relationship between usage conflict and intention to use will vary depending on experience of using biometric media.

3.3 Operational Definitions of Variables and Measurement Tools

Independent variables of this research are Information privacy risk, Privacy concern, Negative Mass media, and Routine seeking personality. The mediating variable is Usage conflict, and the dependent variable is Intention to Use, and moderating variable is Experience of using biometrics.

The questionnaire used in this research consisted of 27 questions, and respondents were asked to mark answers on Likert-type 7-point scale. Operational definitions of variables, measurement items, and related researches are summarized in Table 2.

4. Empirical Analysis

4.1 Data Collection and Analytical Method

To achieve the research aim, the survey was conducted to 308 users for a month from December 2 to December 30, 2015.

Collected data were analyzed using SPSS 22.0 and AMOS 22.0. First, to examine demographic characteristics of respondents, frequency analysis was done using SPSS 22.0. And, based on factor analysis on variables, reliability and validity tests were done. And, to examine causal relations among variables suggested in this research, structural equation model analysis was performed with AMOS 22.0.

4.2 General Characteristics of the Sample

Frequency test on demographic characteristics of respondents led to the followings. 208 (67.5%) were males, and 100 (32.5%) were females. Age group distribution was as follows: 40s - 117 (38.0%); 30s – 89 (28.9%); 20s – 65 (21.1%); 50s or over – 37 (12.0%). Job categories of respondents were as follows: office workers – 180 (58.4%); college or graduate school students – 42 (13.6%); government officials – 31 (10.1%); professionals 26 (8.4%); self-employed – 14 (4.5%); researchers – 8 (2.6%), housewives – 5 (1.6%); others 2 (0.6%). School careers of them were as follows: university students or graduates – 202 (65.6%); graduate school students or graduates – 57 (18.5%); technical college students or graduates – 39 (12.7%); high school graduates or lower – 10 (3.2%). 184 (59.7%) had religions and 124 (40.3%) did not. Residential areas of respondents were as follows: Seoul – 131 (42.5%); Gyeonggi province 83 (26.9%); Chungnam/Chungbuk provinces – 58 (18.8%); Gangwon province - 24 (7.8%); Jeju province – 9 (2.9%); Gyeongnam/Gyeongbuk provinces 3 (1.0%). 224 respondents (59.6%) had experience of using biometrics, while 152 (40.4%) did not.

4.3 Test of Measurement Model

To secure convergent validity among variables and perform path analysis, confirmatory factor analysis for variables was performed. As shown in Table 3, standardized loading values were all 0.5 or above, and all average variation estimates (AVE) were also 0.5 or above, proving that the data secured convergent validity. Composite reliability (CR) of each construct concept was 0.7 or above, showing that the data have convergent validity or internal consistency. And, the range of squared multiple correlations (SMC) was 0.564 ~ 0.890, which means that adopted variables contribute to concept explanation.

Next, to evaluate discriminant validity, this research compared correlation coefficients and square root values of AVE. In general, when square root value is bigger than correlation coefficient with other variable, discriminant validity is secured[43]. Table 4 demonstrates that square root

Table 3. Convergent validity and reliability test results of the model

Potential variable	Measurement variable	Unstandardized estimate	Standardized estimate	S.E	t-value	SMC	CR	AVE
Information Privacy Risk	IPR 1	1	.909	-	-	.826	.834	.501
	IPR 2	1.024	.936	.036	28.563	.876		
	IPR 3	.954	.888	.039	24.640	.789		
	IPR 4	.903	.867	.039	23.179	.751		
	IPR 5	.794	.825	.038	20.728	.680		
Privacy Concern	PC 1	1	.910	-	-	.827	.853	.593
	PC 2	1.002	.929	.036	28.048	.863		
	PC 3	1.043	.923	.038	27.497	.852		
	PC 4	1.047	.905	.040	26.026	.820		
Negative Mass Media	NMM 1	1	.836	-	-	.700	.818	.530
	NMM 2	1.091	.881	.056	19.628	.776		
	NMM 3	1.146	.926	.054	21.239	.857		
	NMM 4	1.020	.864	.054	19.001	.746		
Routine Seeking Personality	RSP 1	1	.859	-	-	.738	.749	.500
	RSP 2	1.026	.925	.054	18.872	.856		
	RSP 3	.868	.751	.057	15.312	.564		
Usage Conflict	UC 1	1	.864	-	-	.746	.884	.561
	UC 2	1.001	.843	.050	19.850	.710		
	UC 3	.950	.833	.049	19.452	.695		
	UC 4	1.115	.908	.048	23.051	.825		
	UC 5	1.145	.944	.046	25.125	.890		
	UC 6	1.151	.943	.046	25.063	.888		
Intention to Use	IU 1	1	.911	-	-	.829	.906	.707
	IU 2	.994	.936	.035	28.293	.876		
	IU 3	1.021	.899	.040	25.276	.807		
	IU 4	.974	.900	.038	25.351	.809		
fit:χ^2=903.486(df=284), χ^2/df=3.180, TLI=.922≧.9, CFI=.932≧.9, RMSEA=.084 ≦.10								

values of AVE are bigger than correlation coefficients, proving that the model secures discriminant validity.

4.4 Test of Structural Model

In the Structural Equation Modeling (SEM), goodness of fit was judged based on TLI, CFI, and RMSEA. If TLI and CFI are .90~.95, and RMSEA is lower than .05, the SEM is evaluated as having good goodness of fit, if RMSEA is in the range of .05~.08, as proper goodness of fit, and, if RMSEA is in the range of .08~.10, as average goodness of fit[44].

To test hypotheses set through path coefficients acquired structural equation modeling, this study evaluated goodness of fit of the modeling on the relationship among variables. The results were χ^2=689.547(df=288), andχ^2/df=2.39, lower than criterion 3.0. TLI=.894 and CFI=.893, somewhat lower than criterion .90. RMSEA=.098, lower than criterion .1. Considering major indices used as evaluation criteria, Even if TLI and CFI values do not satisfy recommended criteria, they do not deviate far from recommended criteria. And, considering that, in structural equation modeling, it is difficult to get goodness of fit indices which are satisfactory in all aspects[45], the goodness of fit of this model can be said to be proper.

Table 4. Discriminant validity analysis results

	AVE	(A)	(B)	(C)	(D)	(E)	(F)
(A) Information Privacy Risk	.501	.708					
(B) Privacy Concern	.593	.695	**.770**				
(C) Negative Mass Media	.530	-.152	-.149	**.728**			
(D) Routine Seeking Personality	.500	.254	.237	-.169	**.707**		
(E) Usage Conflict	.561	.653	.647	-.029	.380	**.749**	
(F) Intention to Use	.707	.651	.650	-.023	.363	.689	**.841**

(Note) Values on the diagonal line are square root values of AVE, and values below them are correlation coefficients.

Table 5. Hypothesis test results

Path					Unstandardized coefficient	Standardized coefficient	S.E.	t-value	Result
H1	IPR	→	UC	+	.145	.179	.152	.952	Reject
H2	PC	→	UC	+	.410	.515	.155	2.652**	**Accept**
H3	NM	→	UC	+	.002	.001	.070	.023	Reject
H4	RSP	→	UC	+	.215	.222	.065	3.295***	Accept
H5	UC	→	IU	-	-.593	-.611	.084	-7.100***	Accept

*p<.05, **p<.01, ***p<.001

The results of hypotheses through path significance of the research model are summarized in Table 5. In this model, usage conflict has explanatory power of 56.1% variation, and intention to use has that of 37.3% variation.

Next, to test H5 and H7, that is, to test moderating effect of experience of using biometric media, this research used the corresponding parameter difference method. To test moderating effect by comparing corresponding parameters, goodness of fit of the whole model should be secured. Then, goodness of fit of each group is checked. Then, cross-validation of two groups is examined by checking b1 ~ b5 variables in paths of each group, and differences in b1 ~ b5 values in each group matrix. The difference between two parameters can be seen as z statistics. If the difference between two parameters is over ±1.96, or over ±2.58, it has moderating effect at significance level α=.05, or α=.01 [46].

As the goodness of fit of the whole model was secured, the respondents were divided into two groups: those who have experiences of using biometric devices (N=161) and those who do not (N=147). The goodness of fit for the former group was χ^2=709.254(df=288), χ^2/df=2.46, TLI=.908, CFI=.919, RMSEA=.096, satisfying all the required criteria.

The goodness of fit for the latter group was χ^2=689.547(df=288), χ^2/df=2.39, TLI=.894, CFI=.893, RMSEA=.098. Though TLI and CFI indices do not satisfy the criteria a little bit, they do not make serious problem in analyzing data. Next, difference of parameters was checked by comparing labels of two groups. The difference was less than ±1.965, making us to reject the moderating effect of experience of using general biometric media. The results of moderating effect test of experience of general biometric media are shown in Table 6.

Even if the moderating effect of using general biometric media failed to secure statistical significance, it was found that, except for the case of information privacy risk, the former group has higher path coefficients in all

Table 6. Test results of the hypothesis that Experience of Using Biometrics has moderating effect

Path					Unstandardized coefficient	S.E.	t-value	P value	Label	Difference between parameters	Result
H5	IPR	→	UC	Y	.047	.210	.224	.823	b1_1	.376	Reject
				N	.145	.152	.952	.341	b1_2		
	PC	→	UC	Y	.532	.233	2.283	*	b2_1	-.438	
				N	.410	.155	2.652	**	b2_2		
	NM	→	UC	Y	.164	.076	2.161	*	b3_1	-1.580	
				N	.002	.070	.023	.982	b3_2		
	RSP	→	UC	Y	.277	.084	3.294	***	b4_1	-.578	
				N	.215	.065	3.295	***	b4_2		
H7	UC	→	IU	Y	-.527	.055	-9.634	***	b5_1	-.667	Reject
				N	-.593	.084	-7.100	***	b5_2		

*p<.05, **p<.01, ***p<.001

the other paths than those of the latter group. That is, we can guess that the group which has experience of using biometric media is less influenced by privacy concern, negative mass media, and routine seeking personality than the group which did not have such experiences. On the other hand, it was found that in the relationship between information privacy risk and usage conflict, the former group had stronger effect, which seems that the former group responds more sensitively to information privacy risk.

5. Research Results and Significances

5.1 Summary of Research Results and Discussions

This research empirically analyzed relationship among perceived risk characteristics (Information Privacy Risk, Privacy Concern, Negative Mass Media), Routine Seeking Personality and Usage Conflict, relationship between Usage Conflict and Intention to Use, and moderating effect of experience of using general biometric media. Major findings and consequent significances of the research can be summarized as follows.

First, it was found that information privacy risk does not have significant effect on usage conflict. The finding is consistent with the research of[10] which argued that real risk does not have effect on user's behavior unless the user does not directly feel risky.

Second, privacy concern was found to be an important element causing usage conflict. It is consistent with the finding of[29] who found that in e-commerce the higher privacy concern is, the lower the intention to participate in e-commerce. That is, the worry of users providing their biometric information in the use of biometric technology boosting convenience compared with identification card has effect on usage conflict of the biometric system.

Third, it was found that negative message through mass media does not have significant effect on usage conflict of the biometric system. The finding is inconsistent with those of previous researches such as the research of[33] that based on impression formation theory, people pay more attention on negative message than on positive message, and the finding of[19] that mass media highlighting negative aspect of SNS can lead to SNS usage conflict. The finding of this research means that negative message of mass media is not strong enough to cause usage conflict. It is in the same context with[15] who argued that mass media are efficient means to boost recognition to specific objects and communication rather than changing people's attitude by persuasion.

Forth, the more one tends to seek routine, the more he or she feels usage conflict. The finding seems to be consistent with the findings of[18] that the higher one's tendency to seek routine, the higher his or her psychological resistance. Users who hate old habits against change are reluctant to change to convenient biometric media.

Fifth, biometric system usage conflict was found to have negative effect on Intention to Use. In other words, psychological dissonance meaning conflict can have negative effect on intention to use the biometric system. It supports the view of[37] who suggested cognitive dissonance theory.

Finally, there was no significant moderating effect of experience of using general biometric media. Whether one experienced using authentication media (fingerprint, iris, finger vein, etc.) in entering or exiting facilities and dealing with documents in public offices except for in financial transactions does not have moderating effect on usage conflict or intention to use the biometric system. It seems that such experiences do not work as motive to use the biometric system in financial transactions (simplified settlement, deposit and withdrawal of money, and transfer, etc.).

5.2 Significances of the Research and Future Research Direction

Theoretical and practical significances of this research are as follows.

First, this is the research on biometrics-based non face-to-face authentication system in financial transactions from the perspective of users rather than from currently popular software engineering approach on biometric technology. More researches on this line are necessary in the future.

Second, now financial institutions make various efforts to make relations with customers more efficient by adopting a new channel system. They need to make continuous effects to strengthen financial security and personal information security, secure a biometric system superior in protecting security, and continue to persuade customers on the convenience and security reliability of the biometric system.

This research has some limits.

First, this research is a research on all kinds of non face-to-face channels (digital kiosk, ATM, smartphone, and Internet banking, etc.). Each channel has unique characteristics. So, if the research had tried to analyze differences derived from different channels, this research would provide more implications.

Second, there are various kinds of biometric technology (fingerprint, iris, palm vein, and face, etc.) for authentication. In spite of differences derived from each biometric technology, this research treated them without differentiating them.

6. Acknowledgment

This research was financially supported by Hansung University.

7. References

1. KFTC 'Biometric Distribution' Standard. Available from: http://www.dt.co.kr/contents.html?article_no=2016010602101460812001, Date accessed: 01/05/2016.
2. Security cards, OTP abolish duty use, Blooming Fintech Era. Available from: http://news.donga.com/3/all/20160221/76584935/1. Date accessed: 02/21/2016.
3. Miller B. Everything you need to know about biometric identification. Personal Identification News Biometric Industry Directory. Werfel & Miller, Inc. Washington DC. 1989; . p.5-8.
4. Way man J. A definition of biometrics National Biometric Test Center Collected Works 1997–2000.San Jose State University. 2000.
5. Coventry L, Angeli A D, Johnson G. Usability and biometric verification at the ATM interface SIGCHI conference on Human factors in computing systems, USA, 2003, . p.153-60.
6. Lee BY, Kim MY. Factors affecting the continuance usage intention of biometric technology: Comparing dark scenario with bright scenario. Journal of Society for e-Business Studies. 2011; 16(3):1-22.
7. Taha K E, Norrozila S. A survey of multi-biometrics and fusion levels. Indian Journal of Science and Technology. 2015; 8(32): 1-10.
8. Oh DY. Biometric-Based authentication system of financial security. Digital Daily Financial IT Innovation 2015 Seminar Presentations. 2014.
9. KB Financial Group Inc. Status and prospects of utilizing biometric technology in the financial industry. KB Knowledge Vitamin. 2014; 14-42.
10. Park YS, Han MH. The effects of perceived risk and perceived quality on the consumer`s online buying behavior. Journal of Korean Marketing Association. 2001; 16(1): 59-84.
11. Dinev T, Hart P. Internet privacy concern and their antecedents-measurement validity and a regression model. Behavior and Information Technology. 2004; 23(6): 413-22.
12. Jang SH. Privacy risk of social network service and user resistance. Master's thesis. Department of Incheon university management. 2014.

13. Lee YN, Kwon OB. Model based approach to estimating privacy concerns for context-aware services. Journal of Intelligence and Information Systems. 2009; 15(2): 97-111.
14. Gatignon H, Robertson T S.A propositional inventory for new diffusion research. Journal of Consumer Research. 1985;11(1): 849-67.
15. Rogers E M. Diffusion of Innovation, 4th (edn). New York :The Free Press;, 2003.
16. Managing Change in the Workplace. https://www.entrepreneur.com/article/275678. Date Accessed: 2016.
17. Tichy N M. Managing strategic change: Technical, political and cultural dynamics., New York: John Wiley& Sons;, 1983.p.434.
18. Kim JJ, Park KK. A study on the relation between personal characteristics and psychological resistance to change & organization commitment. Korean Journal of Industrial and Organizational Psychology. 2008; 21(3): 429-50.
19. Park KJ. A Study on the avoidance intention of social network service in post adoption context: Focusing on the Facebook user. The Journal of Information Systems. 2015; 24(1): 147-68.
20. Sweeney J C, Soutar G N.Are there cognitive dissonance segment?Australian Journal of Management. 2003; 28(3): 227-49.
21. Krueger N. The cognitive infrastructure of opportunity emergence. Entrepreneurship Theory and Practice. 2000; 25(3): 5-23.
22. Davis FD. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly. 1989; 13(3): 319-40.
23. Davis FD, Bagozzi RP, Warshaw PR. User acceptance of computer technology: A comparison or two theoretical model. Management Science. 1989; 35(8): 982-1002.
24. Venkatesh V, Davis F D. A theoretical extension of the technology acceptance Model: Four longitudinal field studies. Management Science. 2000; 46(2):186-204.
25. Lim J S. A study on the effect of the introduction characteristics of cloud computing services on the performance expectancy and the intention to use: Focusing on the innovation diffusion theory.[PhD thesis]. Dan Kook University; 2012.
26. Shin MS, Han SS, Kim HJ. The effect of perceived risk, service quality and individual tendency on trust, satisfaction & continuous use intention., Management Education Review., 2012; 27(1): 1-23.
27. Kim J h, Sung B K, Bu S H.The influence of usefulness, convenience & privacy threats on accepting online behavioral advertising: Focused on consumer`s psychological response & perceived controllability. The Korean Journal of Advertising. 2010; 87: 263-302.
28. Lee MN, Sim JW. The moderating effect by gender in the relationship between the perception of online privacy and use of privacy protection dtrategy. Media, Gender & Culture. 2009; 12: 165-90.
29. Liao. Examining the impact of privacy. Trust and risk perceptions beyond monetary transactions: An integrated model. Electronic Commerce Research and Applications. 2011;10(6): 702-15.
30. Ki SJ, Lee SY. Exploring categories of SNS user on the basis of privacy concern and delf-efficacy. Korean Journal of Journalism & Communication Studies. 2013; 57(1): 81-110.
31. Hyuk I, Seong T P, Ko M H.A study of factors that affect the right to be forgotten and self-disclosure intent in SNS. Indian Journal of Science and Technology. 2016; 9(26): 1-8.
32. Hong JP. Conceptual investigation of differential functions of advertising and publicity: Focusing on consumers` motivation, opportunity and sbility to process persuasive messages. Korean Journal of Consumer and Advertising Psychology. 2006; 7(1):47-73.
33. Jeon SR, Park HJ. The influence of information characteristics on word-of-mouth effect. Journal of Consumer Studies. 2003; 14(4):21-44.
34. Kim JH, Bu SH. The effect of scarcity message on purchasing intention in message framing of advertising. Korean Journal of Consumer and Advertising Psychology. 2007; 8(2):183-203.
35. Oreg S. Resistance to change: developing an individual differences measure. Journal of Applied Psychology. 2003; 88(4):680-93.
36. Bartunek JM, Moch MK. First-order, Second-order and third-order change an organization development intervention: A cognitive approach. Journal of Applied Behavioral Science. 1987;28(4):204-23.
37. The theory of Cognitive Dissonance. http://www.simply-psychology.org/cognitive-dissonance.html. Date Accessed: 2008.
38. Suh MS, Ahn JW, Lee EK, Oh DY. Purchasing avoidance of digital convergence products: Focusing on the customer's psychological factors and the innovation resistance. Korean Journal of Contents. 2009; 9(1):270-84.
39. Park KJ, Park S B.A study on the stress of using social networking services and its discontinuance intention. Journal of the Korea Society of Computer and Information. 2014; 19(12):275-86.
40. Dinev T, Hart P. An extended privacy calculus model for E-commerce. Information System Transactions Research. 2006; 17(1):61-80.
41. Lee H S, Lim D W, Jung ZH. Personal information overload and user resistance in the big data age. Journal of Intelligence and Information Systems. 2013;19(1):125-39.
42. Bhattacherjee A. Acceptance of e-commerce services: the case of electronic brokerages. Systems, Man and Cybernetics, Part A: Systems and Humans. IEEE Transactions on., 2000;, 30(4): 411-20.

43. Fornel C, Larcker DF. Structural equation models with unobservable variables and measurement error: Algebra and statics. Journal of Marketing Research., 1981; 25(2): 186-92.
44. Barbara S. The criteria for selecting appropriate fit indices in structural equation modeling and their rationales. Korean Journal of Clinical Psychology. 2000; 19(1):. 161-77.
45. Gefen D, Stuab DW, Boudreau MC. Structural equation modeling and regression: Guidelines for research practice. Communications of the Association for Information Systems. 2000; 4(7):1-76.
46. Bae B R. AMOS 19 Structural equation modeling - Principles and Practices, 3 rd (edn). New York: THE GUILFORD PRESS; 2011.