International Journal of Engineering Sciences & Emerging Technologies, Dec. 2024
ISSN: 22316604 Volume 11, Issue 4, pp: 1099-1107 ©IJESET

THE EFFECT OF INNOVATION RESISTANCE AND FACE RECOGNITION PAYMENT SYSTEM FEATURES ON INTENTION TO USE

Mohd Salman[1], Rahul Kumar Mishra[2]

[1]IFTM University, Moradabad, India.
salmank64@gmail.com

[2]IFTM University, Moradabad, India.
rahulmishra@iftmuniversity.ac.in

ABSTRACT

New technologies brought forth by the fourth industrial revolution, such facial recognition, have greatly improved customer convenience by being implemented in a variety of industries, including customs, attendance, and payment systems. Face recognition payment services have emerged as a result of the financial industry's recent use of this technology. In under five seconds, transactions are completed with this approach, which scans a person's face, analyses important facial traits, and compares the data with recorded information to verify identity. By examining the features of settlement systems and innovation resistance, this research seeks to comprehend the uptake of face recognition payments and any opposition to their application. Contactless transactions, dependability, security, and convenience are all provided by the facial recognition payment system. Using Smart partial least squares 2.0 structural equations to assess a survey of Chinese consumers, the following outcomes were obtained: User innovation resistance is adversely connected with system convenience, dependability, and security. On the other hand, the system's contactless feature helps reduce users' aversion to innovation.

KEYWORDS: *Face Recognition, Data Base Management System, SQL Query Language*

1. INTRODUCTION

The fourth industrial revolution ushered in advancements in big data, AI, IoT, cloud computing, and blockchain, rapidly applied across sectors. Fintech, especially, underwent profound changes with these technologies, significantly reshaping the payment industry. The launch of the online payment service "PayPal" in 1998 marked the beginning of the convenient payment industry. Mobile settlement services divided into online remote and short-distance categories as mobile devices became more sophisticated. Online remote settlement concentrates on digital transactions, whereas short-distance settlement involves scanning barcodes or QR codes at physical establishments. Fast online identity authentication using short passwords or biometric techniques like fingerprint or facial recognition on smartphones has made Quick Online Identity (Fido) technology popular. The development of smartphones has propelled this transition, resulting in the rapid expansion of the mobile simple payment industry. According to Statista data, the value of mobile settlements worldwide increased from $45 billion in 2014 to $108 billion in 2019.

The advancement and integration of technologies like the Internet of Things and artificial intelligence have given rise to a novel and straightforward payment solution. In 2013, Finland took the lead by introducing "Uniqul," the first face recognition payment system in history. In 2018, Alibaba's Alipay launched "Ching-ting," a face-recognition payment system, in response. In 2019, Shinhan Bank of South Korea introduced its facial recognition payment service, following suit. This marks the onset of an era where facial recognition enables seamless payments, freeing users from reliance solely on mobile phones. Even in scenarios where mobile phones are unavailable or powered off, users can still execute payments using camera of (POS) integrated with the face recognition payment system. Nonetheless, as electronic financial transactions proliferate, service providers must amass substantial amounts of personal data to enhance user convenience and satisfaction. Users are required to consent to the collection of personal information to utilize this service. Consequently, in the age of big data, there's a heightened risk of personal information breaches. This underscores the notion that while convenience expands, so too does the associated risk.

Face recognition technology has become ubiquitous across various domains, leading to widespread collection of human biological information. However, concerns persist regarding the secure storage, transmission, and utilization of this data. Unlike other forms of biometric data, such as fingerprints, faces are constantly exposed to public environments and are inherently difficult to conceal or alter. This has sparked fears among individuals that their facial information may be captured by cameras equipped with facial recognition technology without their consent, potentially resulting in information leaks and significant risks and damages. Consequently, while the emergence of face recognition payment services heralds the advent of a new payment market, its maturity and reliability are often called into question due to these apprehensions.

2. PAYMENT SYSTEMS USING FACE RECOGNITION TECHNOLOGY

It functions by automatically detecting and analyzing facial features within input images or videos to determine the identity of a person [2]. This technology operates similarly to other forms of identity recognition such as ID card, fingerprint, and iris recognition. During face recognition, a camera captures an individual's face, which is then analyzed to extract facial features like eyes, mouth, and ears. This data is subsequently compared with stored databases, utilizing pattern recognition techniques. Various methods, including thermal imaging, ultraviolet rays, or three-dimensional measurements, are employed to extract facial features. Modern face recognition systems leverage deep learning algorithms, significantly enhancing recognition accuracy. As a result, these systems find widespread applications in fields such as healthcare, government, and retail. Moreover, the COVID-19 pandemic has led to a surge in the utilization of face recognition systems, with applications such as temperature monitoring and access control becoming increasingly common. With a predicted cumulative annual growth rate (CAGR) of 16.6%, the global face recognition industry is expected to increase from $3.2 billion in 2019 to $7.9 billion by 2024. According to data from the Prospective Industry Research Institute, China accounts for 15% of the worldwide face recognition market. The face recognition market in China was estimated to be worth 2.51 billion yuan in 2018 and is predicted to grow to over 10 billion yuan by 2024.

Face recognition payments are often made through two primary services. The first is mobile easy payment, a mobile phone service that uses facial recognition in place of password input to confirm the identity of the user during transactions. First introduced in July 2013, the second is a face recognition-based payment platform, created by the Finnish firm "Uniqul". To make payments using this system, users only need to gaze into the point-of-sale (POS) screen's camera.

3. FEATURES OF THE FACE RECOGNITION PAYMENT SYSTEM

Pattern recognition and computer vision studies have benefited greatly from face recognition technology. In order to identify people, it automatically recognizes and evaluates facial traits in still photos or videos. Similar to other forms of identity recognition such as ID card, fingerprint, and iris recognition, face recognition involves scanning an individual's face with a camera and analyzing it into distinct facial feature points like eyes, mouth, and ears, from which data is extracted. This data is then compared with stored databases using pattern recognition techniques to determine identity. Various methods, including thermal imaging, ultraviolet rays, or three-dimensional measurement, are employed to extract facial features. Deep learning algorithms are commonly utilized in face recognition systems, significantly enhancing recognition accuracy. Consequently, these systems find widespread applications in fields such as healthcare, government, and retail. Moreover, the COVID-19 pandemic has fueled an increase in the deployment of face recognition systems, including those for body temperature monitoring and access control measures.

To enhance convenience, face recognition providers often gather extensive personal information. However, in the absence of unified regulations governing big data's usage rights, ownership, and other pertinent issues, the risk associated with amassing large volumes of human data in the field of data continues to escalate. Consequently, individuals are increasingly hesitant to embrace facial recognition technology for payment purposes. Two common services facilitate payments through facial recognition. Firstly, there's mobile simple payment, a mobile phone-based service that employs the device's camera to recognize the owner's face, replacing the need for password input during transactions [5]. The other service is a payment platform built upon facial recognition systems, pioneered by the Finnish startup "Uniqul" in July 2013. Here, customers simply look at the camera on the point-of-sale (POS) screen during payment. To utilize this system, consumers must first link their facial information with their personal account. Upon facial recognition verification, payments are deducted from the associated account, enabling transactions to be completed within a mere five seconds. This method primarily serves offline payment purposes.

4. FACE RECOGNITION PAYMENT SYSTEMS ENCOMPASS SEVERAL KEY ASPECTS

4.1. Convenience

These systems provide a hassle-free alternative to traditional payment methods, eliminating the need for physical cards or passwords. Users can swiftly authenticate transactions using their facial features, streamlining the payment process.

4.2. Security

Face recognition payment systems offer heightened security through biometric authentication, which is unique to each individual. This reduces the risk of identity theft and fraudulent activities, as facial features are challenging to replicate or deceive.

4.3. Reliability

Advancements in technology have bolstered the reliability of face recognition systems, ensuring accurate identification of individuals. This reliability fosters confidence in the system's ability to process transactions securely and efficiently.

4.4. Non-contact

Face recognition payment systems facilitate contactless transactions, minimizing physical interaction between users and payment terminals. This feature is especially valuable in situations where hygiene and safety are paramount, such as during the COVID-19 pandemic.

5. THE RESEARCH MODEL AND HYPOTHESES FOR A STUDY ON FACE RECOGNITION TECHNOLOGY IN PAYMENT SYSTEMS

5.1. Research Model

- Independent Variables
- ✓ Convenience of Face Recognition Payment System.
- ✓ Security of Face Recognition Payment System.
- ✓ Reliability of Face Recognition Payment System.
- ✓ Perceived Risk of Personal Information Collection.

ISSN: 22316604 Volume 11, Issue 4, pp: 1099-1107 ©IJESET

- Dependent Variable
- ✓ Intention to Use Face Recognition Payment System.

5.2. Research Hypotheses

- Security of the face recognition payment system positively influences the intention to use it.
- Reliability of the face recognition payment system positively influences the intention to use it.
- Perceived risk of personal information collection negatively influences the intention to use the face recognition payment system.

These hypotheses posit that factors such as convenience, security, and reliability of face recognition technology positively impact users' intention to adopt it for payment purposes, while perceived risks associated with personal information collection may negatively influence their intention to use it.

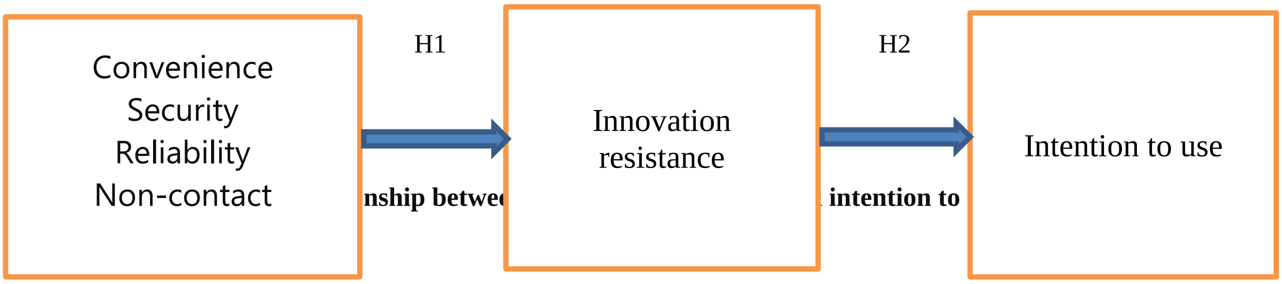

Fig. 1: Relationship between innovation resistance and intention to use

In the context of face recognition technology in payment systems, it can be posited that individuals who harbor higher levels of innovation resistance may exhibit greater uncertainty and doubt regarding the adoption of this novel payment method. This uncertainty could lead to hesitancy in communicating about the technology and ultimately influence their intention to use it.

Hypothesis The intention to use new face recognition technology in payment systems is adversely affected by innovation resistance. This hypothesis posits that individuals with elevated levels of innovation resistance are less inclined to adopt face recognition technology for payments.

H1 suggests that their resistance arises from uncertainties and suspicions regarding the changes brought about by the new technology, ultimately causing them to reject its adoption.

H2 asserts that innovation resistance has a negative influence on the intention to use face recognition technology in payment systems.

6. THE OPERATIONAL DEFINITIONS AND POTENTIAL MEASUREMENTS FOR THE VARIABLES

let's outline the operational definitions and potential measurements for the variables in tabular format:

Table 1. The operational definitions and potential measurements

Variable	Operational Definition	Measurement
Innovation Resistance	The degree of uncertainty and doubt individuals have towards adopting new technology innovations.	- Resistance to change scale - Perceived risk scale - Attitude towards technology scale

Intention to Use	The willingness or likelihood of individuals to use face recognition technology in payment systems.	- Likert scale (e.g., strongly agree to strongly disagree) - Behavioral intention scale (e.g., likelihood of using the technology in the future)

7. ANALYSIS OF THE RELATIONSHIP BETWEEN INNOVATION RESISTANCE AND INTENTION

The empirical analysis of the relationship between innovation resistance and intention to use face recognition technology in payment systems, you could conduct a survey or experiment to gather data from potential users.

The survey targeted Chinese consumers and commenced on August 19, 2020, spanning a duration of 21 days, during which 198 responses were collected. Among the respondents, males constituted 46.46% while females comprised 53.54%. The largest demographic group fell within the 20-29 age bracket, representing 43.94% of the sample. Additionally, individuals with undergraduate-level education accounted for 82.83% of respondents, with students constituting 40.91% of the surveyed population. Given that younger consumers tend to be more receptive to adopting innovative technology products, this analysis primarily focuses on individuals aged 20 to 29 with a college degree or higher.

Here's a general outline of the steps you could take:

Survey Design: Develop a questionnaire that includes items to measure innovation resistance and intention to use face recognition technology. Ensure that the questions are clear, concise, and relevant to the research objectives.

Sampling: Determine the target population for your study and select a sample that is representative of this population. Consider factors such as demographics, geographic location, and technological literacy.

Data Collection: Administer the survey to the selected sample either online, through face-to-face interviews, or other suitable methods. Ensure that participants understand the instructions and provide informed consent to participate.

Table 2. Demographic Characteristics

Item		**Frequency**	**Ratio(%)**
Gender	**Male**	93	47.60
	Female	105	52.90
Age	**10-19**	41	21.10
	20-29	88	42.50
	30-39	55	27.43
	40 -49	5	2.50
	Over 50	3	1.01
Education	**Below high school**	3	1.50
	Graduated from high school	16	7.89
	University graduation	165	83.01
	Master's degree	12	5.89
	PhD or above	8	4.21
Job	**Profession**	42	21.23
	Self-employment	17	8.05
	White collar	38	19.67
	Student	84	44.47
	Other	20	12.21

Data Analysis: Following the collection of survey responses, the relationship between innovation resistance and intention to use can be investigated by statistically analyzing the data using techniques like correlation analysis, regression analysis, or structural equation modeling (SEM). To assess the validity and reliability of the research model, a measurement model analysis must be done prior to doing structural equation analysis.

Reliability Analysis: Calculate Cronbach's Alpha for each construct in SPSS to assess internal consistency reliability. Ensure that all values are 0.7 or higher, indicating satisfactory reliability

Validity Analysis: Use Smart PLS 2.0 to calculate factor loading values, CR, and AVE for each construct. Factor loading values should ideally be 0.6 or higher, CR should be 0.7 or higher, and AVE should be 0.5 or higher, indicating convergent validity.

Measurement Model Assessment: Evaluate the measurement model overall to ensure that it adequately represents the constructs and their relationships. This may involve examining fit indices such as the goodness-of-fit (GoF) and standardized root mean square residual (SRMR).

Table 3. Trustworthiness and Internal Coherence

Variable name		Factor Loading	AVE	Composite Reliability	Cronbach's Alpha
Convenience	**CON1**	0.927	0.803	0.925	0.873
	CON2	0.936			
	CON3	0.832			
Reliability	**RES1**	0.924	0.860	0.949	0.920
	RES2	0.947			
	RES3	0.915			
Security	**SEC1**	0.923	0.866	0.952	0.923
	SEC2	0.943			
	SEC3	0.928			
NON Contact	**NOC1**	0.907	0.804	0.892	0.757
	NOC2	0.888			
Innovation resistance	**INR1**	0.934	0.881	0.957	0.933
	INR2	0.960			
	INR3	0.922			
Intention to use	**IOU1**	0.926	0.839	0.940	0.904
	IOU2	0.941			
	IOU3	0.881			

It's great to hear that the analysis confirms discriminant validity for all variables! This indicates that each variable in your research model is distinct from the others, supporting the validity of your measurement model. Moving forwa rd, you can proceed with confidence to conduct structural equation modelling to further explore the relationships between the variables in your study.

Table 4. Relationship between discriminant validity and Correlation

Variable name	AVE	Convenience	Responsibility	Security	Non-contact	Innovation resistance	Intention to use
Convenience	0.803	0.897					
Reliability	0.860	0.813	0.927				
Security	0.866	0.742	0.731	0.930			
Non-contact	0.804	-0.271	-0.284	-0.256	0.897		
Innovation resistance	0.881	-0.536	-0.543	-0.509	0.657	0.937	

Intention to use	0.839	0.808	0.810	0.820	-0.330	-0.535	0.916

8. CONFIRMATION OF THE STRUCTURAL MODEL

In this research, Partial Least Squares (PLS) was chosen as the data analysis method due to several key considerations specific to the study. These include the theoretical robustness of PLS, the sample size, and the customization of the questionnaire. The fitness of the model is assessed based on the R-squared (R2) value: if R2 is 0.26 or higher, the model exhibits a high degree of fitness; if it falls between 0.26 and 0.13, the fitness level is considered medium; and if it's below 0.13, the fitness is regarded as low.

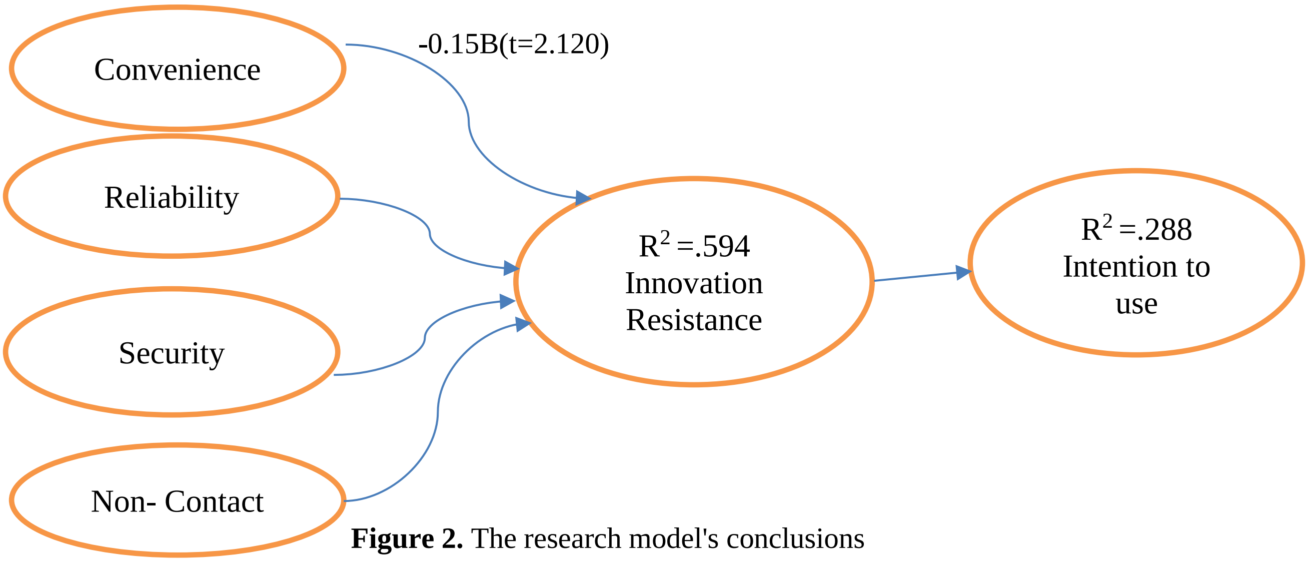

Figure 2. The research model's conclusions

10. THE RESEARCH MODEL ANALYSIS

Table 5. Result of Hypothesis with Intention to use summary

	Cause variable	Result variable	Path coefficient	T-value	Result
H1	Convenience	Intention to use	-0.158	2.120	Accept
H2	Reliability	Intention to use	0.167	2.090	Accept
H3	Security	Intention to use	-0.134	2.041	Accept
H4	Non-contact	Intention to use	0.532	6.255	Accept
H5	Innovation resistance	Intention to use	0.536	6.087	Accept
t=1.960** (P<0.05)					

11. CONCLUSION

This study explores Chinese consumers' acceptance of face recognition payment systems amid China's rapidly evolving market. A broad sample survey across different age groups in China gathered relevant data. Hypothesis 1, focusing on the attributes of face recognition payment systems and innovation resistance, found that convenience, reliability, and security negatively affect resistance, while the non-contact feature positively impacts it. Hypothesis 2, linking innovation resistance with customer intention to use, was similarly supported, showing a negative correlation between the two.

• The study found that facial recognition payment systems' ease of use, dependability, and security greatly reduce opposition to innovation. This suggests that by providing strong security measures, increased convenience, and user confidence, these systems lessen user resistance to embracing new technology.

• The study discovered that a facial recognition payment system's greater non-contact capabilities raises resistance to innovation. This demonstrates how important non-contact qualities are. These devices speed up verification and simplify authentication, but they also make it possible to gather and authenticate face data without making physical contact, which raises questions about illegal data gathering and possible financial losses.

• According to the research findings, adopting behavior is negatively impacted by innovation resistance. To put it simply, people are less likely to adopt new technology or services if they have more reservations, worries, or other types of resistance towards them.

REFERENCES

[1] M. Kim, D. Son, "The Effect of Privacy and Trust Factors in Fintech Service", Korea Internet Electronic Commerce Association, (2020), Vol. 20, No. 1, pp. 87-98.

[2] Ghosh, Ramkrishna. "An efficient and robust modified RSA based security algorithm in modern cryptography." Journal of Computer Science Engineering and Information Technology Research (JCSEITR), Vol. 6, Issue 2, pp, 15-22.

[3] H. Kim, J. Moon, J. Park, "Research Trends for Deep Learning-Based High-Performance Face Recognition Technology", Electronic Communication Trend Analysis, (2018), Vol. 33, No. 4, pp. 43-53.

[4] Bangar, Ashwini, and Swapnil Shinde. "Study and comparison of cryptographic methods for cloud security." International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), Vol. 4, Issue 2, pp, 205-212.

[5] J. Lee, "Changes in Society According to Facial Recognition Technology", Magazine of the SAREK, (2020), Vol. 49, No. 3, pp. 90-91.

[6] Yuvraj Singh,. "CONCEPTUAL STUDY ON NETWORK SECURITY AND ITS TYPES", International Journal of General Engineering and Technology (IJGET), Vol. 6, Issue 5, pp; 37-42.

[7] "2020 Face Recognition Industry Research Report", China Information Technology Sheet Transformation Technical Committee..

[8] Preeti Patel, "Security of Information with Biometric Applications", IASET: International Journal of Library & Educational Science (IASET: IJLES), Vol. 2, Issue 2, pp, 81-88.

[9] H. Lee, S. Park, M. Sung, C. Sun, M. Jeong, Y. Park, J. Yun, "A Comparison of User Perceptions of User Interface Security Features within Mobile Easy Payment System", The HCI Society of Korea, (2018), pp. 503-511.

[10] Ruchir Bhatnagar & Vineet Kumar Birla, "Wi-Fi Security: A Literature Review of Security in Wireless Network", IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET), Vol. 3, Issue 5, pp, 23-30.

[11] H. Baek, "Status of bio-recognition technology applied to simple payment", Special Report_ Special Theme, (2016), vol. 165, pp. 47~52.

[12] Mudassir Khan & Shameemul Haque, "Cyber Security and Ethics on Social Media", IMPACT: Journal of Modern Developments in Applied Engineering & Technology Research (IMPACT: JMDAETR) Vol. 1, Issue 2, pp, 51-58.

[13] M. Choi, S. Song, "A Study on the Influence of System Quality Characteristics of Mobile Payment Service on Discontinuance Intention", Journal of Korean Social Management, (2018), Vol. 46, No. 3, pp. 625-640.

[14] H. Gao, A Study on Intention to Use Fintech Service: Focusing on Fintech users in Korea and China, Doctoral dissertation, Keamyung University, (2019).

[15] D. Choi, “Analysis and Suggestion of Smartphone Authentication Scheme using Biometrics”, Asiapacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, (2017), vol. 8(1), pp. 875~885.

[16] H. Jang, “A study to Promote Use and Reuse Intention in Electronic Banking Service: Focused on Internet Banking and Mobile Banking”, The Journal of Internet Electronic Commerce Research, (2009), vol. 9(1), pp. 307~330.

[17] H. Kwon, “A Study on Possible Effects of Service Quality in e-Banking and Mobile Banking upon Customer Satisfaction”, Sookmyung Women's University Graduate School of Policy and Industry, Master Thesis, (2008).

[18] G. Chandrika, "Study on Software Reliability and Reliability Testing", Asia-pacific Journal of Convergent Research Interchange, Vol.1, No.1, (2015), pp. 7-20

[19] S. Kim & L. Li, “Factors Affecting the Intention to Use of Smart-Phone Banking Service: A Case of Chinese Users”, Journal of the Korea Contents Association, (2012), vol. 12(11), pp. 303~312.

[20] V. Bhavana, "Data Security in Cloud environments", Asia-pacific Journal of Convergent Research Interchange, Vol.1, No.4, December (2015), pp. 25-31.

[21] J. Bae, “A Study on the Innovation Resistance and Deactivating Factors of Internet of Things (IoT) Services: Focusing on the In-depth Interview Method”, The e-Business Studies, (2017), vol. 18(2), pp. 289~300.

[22] Y. Zhang, J. Ma, H, Park, “Factors Affecting the Usage of Face Recognition Payment Service”, Journal of the Korea Contents Association, (2019), Vol. 19, No. 8, pp. 490-499..

[23] J. Shin, S. Lee, “A Study of Intention to Use Wrist-worn Wearable Devices Based on Innovation Resistance Model - Focusing on the Relationship between Innovation Characteristics, Consumer Characteristics, and Innovation Resistance”, Journal of the Korea Contents Association, (2016), Vol. 16, No. 6, pp. 123-134.

[24] S. Yang & H. Shin, “Innovation Resistance of Consumer in Accepting New Technology - With Emphasis on Mobile Phone Touch Interface Technology-”, Design Studies, (2010), Vol. 23, No. 3, pp.37-52.

[25] G. Jang, H. Jang, “The Relationship of Mobile Payment Service Using Value and Innovation Resistance, Continuous Use Intention”, Journal of Digital Contents Society, (2018), Vol. 19, No. 11, pp. 2203-2210.