Exploring the Continuous Learning Willingness Under the Risk of Data Breach in Online Learning System: A Fuzzy-Set QCA Approach

Yuwei Jiang
School of Educational Information Technology
Central China Normal University
Wuhan, China
614957476@qq.com

Qingtang Liu
School of Educational Information Technology
Central China Normal University
Wuhan, China
liuqtang@mail.ccnu.edu.cn

Shufan Yu
School of Educational Information Technology
Central China Normal University
Wuhan, China
yushufan1993@gmail.com

Jingjing Ma
School of Educational Information Technology
Central China Normal University
Wuhan, China
2503880567@qq.com

Linjing Wu
School of Educational Information Technology
Central China Normal University
Wuhan, China
wlj_sz@126.com

***Abstract*—With the rapid popularization of online learning systems, the impact of data breach risk on the willingness to continue learn in online learning systems has become the focus of attention. Based on the privacy calculus theory, four influencing factors were proposed: risk perception, benefit perception, trust perception and privacy perception. Qualitative comparative analysis (QCA) was used to conduct configuration analysis on the questionnaire results, and to obtain the configurations of good or poor learning willingness. The results showed that, (i) the learners' perception of the existence of benefit and trust in the online learning system helps to improve continuous learning willingness, but this is not a necessary condition, (ii) risk aversion and preventing privacy breach are the urgent needs of online learning systems. The paper highlights the direction of future efforts for online learning systems from the perspective of data breach.**

Keywords—online learning system, data breach, learning willingness, QCA

I. INTRODUCTION

Online learning systems take advantage of the openness and convenience of modern information technology to share educational resources, change traditional teaching methods, and make online learning a mainstream learning method [1]. In order to maximize the benefits, the online learning system needs to provide rich and personalized functions to attract users, and it is necessary to collect a large number of learners' personal learning information (e.g., content information, behavior information) to achieve this purpose. However, there is a risk of breaching user data in the process.

It can be seen from previous data breach incidents on online systems that the risk of data breach poses a certain threat to the personal and learning information security of teachers and students [2]. A survey on the perception of privacy breach caused by tracking data analysis in online learning, pointed out that perceived data breach can reduce learners' willingness to use the online system [3]. However, many existing studies only consider the effect of a single variable, and there is an interaction relationship between the variables, which together determine the willingness to continue learning.

Based on this, the paper takes the privacy calculus theory as the theoretical basis, adopts the method of questionnaire survey, and conducts data analysis by QCA. A combination of qualitative and quantitative methods is used to find the configuration factors that affect college students' continuous willingness to learn under the risk of data breach in the learning system.

II. RELATED WORK

Privacy calculus theory states that individuals' willingness to disclose information is based on a comparison of expected benefits and expected risks in a given context [4]. The computational form of privacy calculus theory is a risk-benefit analysis. The more benefits people expect, the higher the likelihood of self-disclosure; the more risk people fear, the lower the likelihood of self-disclosure. Focusing on e-learning systems, fear of risk reduces willingness to use online services [5]. From a benefit perspective, existing research also shows that perceived usefulness positively affects online learner satisfaction, thereby increasing their willingness to continue using [6]. Studies have shown that, in addition to the consideration of risks and benefits, there is a significant correlation between the degree of trust in online service providers and the willingness to disclose [7]. Therefore, the four factors privacy perception, risk perception, benefit perception and trust perception are summarized to explore the factors that affect the continuous willingness to learn in online learning system.

A. Risk Perception

Risk Perception is defined as a subjective judgment about a particular risk [8]. Most learners make basic judgments about the risks they face before continuing their online learning activities to determine whether the estimated risks are within their tolerance. Risks include online learning systems being attacked, learning and private data being breached, etc. The greater the perceived risk, the more resistance there will be and the less obvious the willingness of learners to learn online.

B. Benefit Perception

Benefit perception is defined as the net benefit in exchange for the cost that consumers perceive to obtain the expected benefit [9]. In the information system, the benefits such as money, efficiency, and personalized functions that users can obtain will often become the main factor in

2022 International Symposium on Educational Technology (ISET) | 978-1-6654-8467-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISET55194.2022.00028

2766-2144/22/$31.00 ©2022 IEEE
DOI 10.1109/ISET55194.2022.00028

that the service can provide. These benefits may be material or spiritual. Many scholars have further determined that the higher the learner's perception of benefits, the higher the learner's satisfaction with the learning system, and the stronger willingness to learn [10].

C. Trust Perception

Trust perception is the reliability of an individual perception system in protecting users' personal information [11]. For online learners, trust perception is the perception of trust in online learning systems, including whether to fulfill the promise of protecting privacy, whether to release sensitive data casually, etc. The trust mechanism of the system is an important factor for learners to generate continuous learning willingness. Online learning individuals are limited by the network due to the lack of shared social background, as well as interpersonal interaction and communication. It reduces learners' perception of trust in learning systems, thereby reducing learners' willingness to learn online independently and collaboratively [12].

D. Privacy Perception

Privacy perception is used to measure an individual's awareness of information privacy [13]. The online learning system data breach is the first to bear the brunt of the breach of private data (e.g., academic performance data, personal sensitive information). The reasons why learning privacy breach affects learners' continuous willingness to learn can be classified as competitive and personal. From a competitive point of view, the learner does not want to let a competitive partner know about his learning. From a personal point of view, the learner wants to hide his personal sensitive information, from the online learning tutor prejudice to reduce anxiety and stress in online learning [14]. Therefore, learner privacy perception is an important influencing factor of online learning behavior willingness. If the degree of privacy perception exceeds the positive benefit perceived by the learner, the system is no longer used for learning [15].

As noted above, risk perception, trust perception, benefit perception and privacy perception all have an important impact on online learning willingness, and the relationship between the factors is mutual influence and inseparable. Therefore, in order to determine the effect of the variables under the influence of each other, QCA was adopted to guide the data collection and analysis.

III. Methodology

A. Participants and Data Collection

The participant is college students in China. The number of valid questionnaires is 204, which is much higher than the sample size required for QCA. All cases were obtained with the consent of the participants. In the basic information of the sample, in terms of gender, boys account for 45.3% and girls account for 54.7%. In terms of majors, science majors account for 55.7%, liberal arts majors account for 24.1%, engineering majors account for 17.7%, and arts majors account for 17.7%, art and sports majors account for 2.5%, which also corresponds well to the proportion of majors in Chinese universities. In terms of grades, students in the four grades account for 26.1%, 20.2%, 23.2%, and 30.5%, respectively. Therefore, the requirement of a certain heterogeneity of the cases is satisfied. And from the final result of willingness to learn, it includes both positive and negative results, which is in line with the analysis requirements of QCA.

B. Scale Design

The scale mainly refers to the existing mature scales, and the relevant wording has been modified to meet the needs of the research. The Cronbach's alpha of the overall scale is 0.809, with high internal consistency. The risk perception dimension is measured by modifying the risk perception dimension in Pavlou et al.'s consumption propensity [16]. The benefit perception dimension is measured using the Lin et al.'s research [17]. The trust perception dimension is measured using the measurement tool of consumers' perception of platform trust in Grazioli et al.'s research [18]. The privacy perception dimension is measured after modifying the measurement items of the perception of privacy security in Workman et al. [19]. The willingness dimension is measured by modifying Milne et al.'s online consumption propensity scale under trust [20].

C. Data Analysis Method

In order to determine the factors that affect the continuous willingness to learn due to the risk of data breach in online learning system, a fuzzy-set QCA method was selected to guide data collection and data classification. QCA is a method that bridges qualitative and quantitative analysis to compare these cases by configuring them to respect the diversity of cases and their heterogeneity in different causally related conditions and contexts. Specifically, it can analyze asymmetric relationships, potential dependencies between conditions, and reveal equivalent configurations for the same outcome. Therefore, QCA goes beyond the limitations of traditional symmetric methods when solving the research problems . The fsQCA3.0 software was used for analysis.

After the selection of conditions and cases, the data will be calibrated in the specific data analysis link. As shown in Equation (1), the direct method of fuzzy-set QCA was used for calibration.

$$y = \text{Calibrate}(x, n1, n2, n3) \quad (1)$$

Where "x" represents the variable that needs to be calibrated, "y" represents the variable after calibration. Define the three qualitative breakpoints as the threshold for full membership (n1), cross-over point (n2), and full non-membership (n3). In the paper, the median +/- standard deviation is used as the full membership or complete non-membership threshold, and the median number is set to cross-over point [21]. See Table I for specific values of each threshold. After calibrating the data, further necessity analysis and configuration analysis are performed.

TABLE I. Data Calibration

Causal conditions/ outcome	M±SD	Qualitative breakpoints		
		n1	*n2*	*n3*
RP	9±2.314	11.314	9	6.686
TP	10±3.101	13.101	10	6.899
BP	11±2.716	13.716	11	8.284
PP	17±5.421	22.421	17	11.579
LW	9±3.323	12.323	9	5.677

[a.] RP risk perception, TP trust perception, BP benefit perception, PP privacy perception, LW Learning willingness

IV. FINDINGS

A. Necessity of Each Single Condition

In order to verify whether the four variables have the necessary conditions to cause high/low continuous learning willingness, a single factor necessity analysis was carried out and the results are shown in Table II. It is generally considered that the condition of consistency $\geqslant 0.9$ (or $\geqslant 0.85$, at least) is a necessary condition. The results showed that there was no necessary condition (consistency < 0.85). There is no single condition variable that can definitely affect the willingness to continue learning. Therefore, further configuration analysis is required to find the configuration that affects the continuous willingness to learn from the perspective of data breach.

We add a '~' before a condition/outcome, it means this condition/outcome does not exist. Conditions connected by '*' exist at the same time, for example BP* ~ PP represents the students have benefit perception without privacy perception.

TABLE II. RESULTS OF NECESSITY ANALYSIS

Causal conditions	High Continuous Learning Willingness		Low Continuous Learning Willingness	
	Consistency	*Coverage*	*Consistency*	*Coverage*
RP	0.428	0.630	0.548	0.596
~RP	0.725	0.685	0.660	0.460
TP	0.735	0.834	0.411	0.345
~TP	0.422	0.492	0.802	0.691
BP	0.717	0.857	0.366	0.323
~BP	0.434	0.481	0.837	0.686
PP	0.527	0.625	0.635	0.557
~PP	0.627	0.699	0.573	0.472

B. Configurations of Continuous Willingness to Learn

Use configuration analysis (standard analysis) to find configurations that affect high/low continuous willingness to learn. Specifically, on the basis of constructing the truth table, in order to simplify the research results, filter out the more extreme cases, and set the frequency cut-off to 2. Also, to maintain a high consistency for each configuration, set the consistency cut-offs to 0.8. The results of analyses using QCA included complex solution, parsimonious solution, and intermediate solution. The intermediate solution was selected in this study, which not only avoids complex and redundant solutions, but also does not violate the facts. The results of the configuration analysis as shown in Table III.

TABLE III. RESULTS OF CONFIGURATION ANALYSIS

Causal conditions	High Continuous Learning Willingness			Low Continuous Learning Willingness	
	A1	*A2*	*A3*	*B1*	*B2*
RP		⊗	●	●	
TP	●		●	⊗	⊗
BP		●		⊗	⊗
PP	⊗				●
Consistency	0.878	0.875	0.820	0.861	0.826
Raw coverage	0.485	0.548	0.349	0.414	0.492
Unique coverage	0.067	0.140	0.081	0.067	0.145
Solution consistency	0.819			0.833	
Solution coverage	0.764			0.559	

[b.] ● stands for the presence of this condition, ⊗stands for the absence of this condition, the space represents that the presence or absence of this condition is irrelevant.

1) Configuration Analysis of High Continuous Learning Willingness: Configuration A1 showed that as long as BP*~PP was satisfied, LW could be caused quasi-sufficiently(consistency=0.878). Since learners want to hide their personal sensitive information, such as test scores, in order to reduce online learning anxiety and stress [14]. During the learning process of the online learning system, if the learner feels that the system better protects the learner's privacy, and at the same time experiences the benefits brought by the system, the learner is willing to use the system for further learning. This is consistent with previous research on online behavioral intentions [22].

Configuration A2 showed that as long as ~RP*TP was satisfied, LW could be caused quasi-sufficiently(consistency=0.875). The reason is that the learners did not perceive obvious risk (e.g., keylogging, identity theft and information sharing related) [23]. At the same, learners have a high degree of trust in the system, and the trust mechanism of the system is an important factor for learners to generate continuous learning willingness [24]. Therefore, learners have the continuous willingness to use.

Configuration A3 showed that as long as RP*BP was satisfied, LW could be caused quasi-sufficiently (consistency=0.820). It shows that even though learners perceive some risks in the system during online learning, they are still willing to continue learning in the virtual learning environment due to the huge benefits brought by the online learning system. On the one hand, compared with the physical environment, learners are more aware of the privacy hazards associated with information sharing in virtual online learning systems [25]. On the other hand, consistent with previous research, most users continue to choose online services because their perceived benefits outweigh their perceived risks [22].

2) Configuration Analysis of Low Continuous Learning Willingness: Configuration B1 and B2 showed that as long as RP*~BP*~TP and ~BP*~TP* PP were satisfied, ~LW could be caused quasi-sufficiently (B1 consistency=0.861, B2 consistency=0.826). Configuration B1 is the same as B2 in that the learner does not perceive the benefits brought by the system and has no sense of trust in the system.The difference is that learners perceive their privacy is breached or various risks of being violated when learning in a virtual environment. In these situations, learners experience lower continuous willingness to learn. It shows that the lack of benefit and trust perception cannot directly lead to the occurrence of low continuous learning willingness, and learners are more concerned about the protection of their own personal safety and the protection of personal privacy information in the process of online learning [26].

V. SUGGESTIONS AND LIMITATIONS

The method of fuzzy-set QCA was used to research the impact of online learning system data breach risk on online college students' continuous willingness learning. A configuration leading to high/continuous learning willingness was finally derived. In view of the results, the following suggestions are scientifically put forward from the perspectives of negative avoidance and positive

improvement: (i) Online learning systems can start from the perspective of reducing system data breach vulnerabilities. From the four links of data collection, circulation, storage and use, the sensitive private information of learners is strictly protected, the risk perception of learners is reduced, the negative impact of online learning is avoided as much as possible, and the safety experience of learners is improved. (ii) Improve learner engagement from a positive perspective, on the one hand, by improving the convenience of the system in terms of time, knowledge, and personalization functions. On the other hand, it has a good privacy protection strategy and a third-party certified privacy seal, and improves the responsibility mechanism to improve the system's reputation mechanism and win the trust of users. In particular, the online learning system needs to improve the learner's sense of benefit. The results found that the enhancement of the sense of benefit can effectively make up for the deficiency brought by the inherent risk perception of online learning.

However, there are still some deficiencies in the paper, and in-depth and comprehensive research is expected to be carried out in the future. Including condition variables are not complete enough, and the scope of research is not broad enough and so on.

ACKNOWLEDGMENT

This work is financially supported by the applied basic frontier project of Wuhan Science and technology Plan (No.2020010601012190), 2020 Key Projects of Hubei Provincial Educational Science Planning (No.2020GA005), and 2021 Teaching Innovation Research Project of the Department of Artificial Intelligence Education, Central China Normal University (No.ZNXBJY202110).

REFERENCES

[1] D. Kim, Y. Lee, W.L. Leite, and A.C. Huggins-Manley, "Exploring student and teacher usage patterns associated with student attrition in an open educational resource-supported online learning platform," Computers & Education, vol. 156, 103961, 2020.

[2] N. Rotem, and R. Locar, "150,000s of e-Learning Students Exposed in 8Belts Data Breach. Security Magazine," June 2020. https://www.securitymagazine.com/articles/92494-000s-of-e-learning-students-exposed-in-8belts-data-breach

[3] M. May, S. Iksal, and C.A. Usener, " Learning Tracking Data Analysis - How Privacy Issues Affect Student Perception on e-Learning," International Conference on Computer Supported Education, Italy, pp. 154-161, 2016.

[4] C. P. K. Armstrong, "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," Organization Science, vol. 10, no. 1, pp. 104-115, 1999.

[5] C. Tu, "The Measurement of Social Presence in an Online Learning Environment." International journal on e-learning, vol. 1, no. 2, pp. 34-45, 2002.

[6] R..Huang, "Overcoming invisible obstacles in organizational learning," Journal of Organizational Change Management, vol. 28, no. 3, pp. 356-368, 2015.

[7] H. Treiblmaier, and S. Chong, "Trust and Perceived Risk of Personal Information as Antecedents of Online Information Disclosure: Results from Three Countries." Journal of Global Information Management, vol. 19, no. 4, pp. 76-94, 2011.

[8] C. Brindley, "Barriers to Women Achieving Their Entrepreneurial Potential: Women and Risk," International Journal of Entrepreneurial Behaviour & Research, vol. 11, no. 2, pp. 144-161, 2005.

[9] Z. Chen, and A. J. Dubinsky, "A conceptual model of perceived customer value in e-commerce: A preliminary investigation," Psychology & Marketing, vol. 20, no. 4, pp. 323-347, 2003.

[10] G. Yang, "Understanding Continuous Use Intention of MOOCs — — A Perspective from Subjective Task Value," Proceedings of 4th International Conference on Social Science and Higher Education(ICSSHE 2018), China, pp. 725-728, 2018.

[11] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," Information Systems Research, vol. 15, no. 4, pp. 336-355, 2004.

[12] H. Tseng, and H. Yeh, "Team members' perceptions of online teamwork learning experiences and building teamwork trust: A qualitative study," Computers in Education, vol. 63, no. 1, pp. 1-9, 2013.

[13] C. Liu, J. T. Marchewka, J. Lu, and C. S. Yu, "Beyond concern – a privacy-trust-behavioral intention model of electronic commerce," Information & Management, vol. 42, no. 2, p.289-304, 2005.

[14] E. Aimeur, H. Hage, and F. Onana, "Anonymous Credentials for Privacy-Preserving E-learning," 2008 International MCETECH Conference on e-Technologies, Canada, pp. 70-80, 2008.

[15] F. Otto, N. A. Badrul, S. Williams, and K. Ø. Lundqvist, "Students' Perception of Privacy Risks in Using Social Networking Sites for Learning: A Study of Uganda Christian University," In E-Learning, E-Education, and Online Training , Italy, pp. 182-190, 2016.

[16] P. A. Pavlou, "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model," International Journal of Electronic Commerce, vol. 7, no. 3, pp. 101-134, 2003.

[17] W.S. Lin, and C.H.Wang, "Antecedences to continued intentions of adopting e-learning system in blended learning instruction: A contingency framework based on models of information system success and task-technology fit," Computers & Education, vol. 58, no. 1, pp. 88-99, 2012.

[18] S. Grazioli, and S. L. Jarvenpaa, "Perils of Internet fraud: an empirical investigation of deception and trust with experienced Internet consumers," IEEE transactions on systems, man, and cybernetics. Part A, vol. 30, no. 4, pp. 395-410, 2000.

[19] M. Workman, W. H. Bommer, and D.W. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test," Computers in Human Behavior, vol. 24. no. 6, pp. 2799-2816, 2008.

[20] G. R. Milne, A. J. Rohm, and S. Bahl, "Consumers' Protection of Online Privacy and Identity," Journal of Consumer Affairs, vol. 38, no. 2, pp.217-232, 2004.

[21] E. J. Douglas, D. A. Shepherd, and C. Prentice, "Using fuzzy-set qualitative comparative analysis for a finer-grained understanding of entrepreneurship," Journal of Business Venturing, vol. 35, no. 1, pp. 1-17, 2020,

[22] Z. S. Byrne, K. J. Dvorak, J. M. Peters, I. Ray, A. Howe, and D. Sanchez, "From the user's perspective: Perceptions of risk relative to benefit associated with using the Internet," Computers in Human Behavior, vol.59, pp. 456-468, 2016.

[23] P.V. Schaik, D. Jeske, J. Onibokun, L. Coventry, J. Jansen, and P. Kusev, "Risk perceptions of cyber-security and precautionary behaviour," Computers in Human Behavior, vol. 75, pp.547-559, 2017.

[24] J. T. Martins, and M. B. Nunes, "Academics' e-learning adoption in higher education institutions: a matter of trust," The Learning Organization, vol. 23, no. 5, pp. 299-331, 2016.

[25] P. Van Schaik, J. Jansen, J. Onibokun, J. Camp, and P. Kusev, "Security and privacy in online social networking: Risk perceptions and precautionary behaviour," Computers in Human Behavior, vol. 78, pp. 283-297, 2018.

[26] A. Majeed, S. Baadel, and A.U. Haq, "Global Triumph or Exploitation of Security and Privacy Concerns in E-Learning Systems," international conference on global security, safety, and sustainability, United Kingdom, pp. 351-363, 2017.