“Sign me in, please!”: An Empirical Study of Federated Identity Threat Avoidance Model

Ari Kusyanti1, a), Harin Puspa Ayu Catherina1, b), Nurudin Santoso1, c) and Popong Effendrik2, d)

1Faculty of Computer Science, Universitas Brawijaya, Jawa Timur 65145, Indonesia.

2Department of Electrical Engineering, Politeknik Negeri Malang, Jawa Timur 65141, Indonesia.

a) Corresponding author: ari.kusyanti@ub.ac.id

b)[harinpuspa@gmail.com](mailto:harinpuspa@gmail.com)

c)[nurudin.santoso@ub.ac.id](mailto:nurudin.santoso@ub.ac.id)

d)popong.effendrik@polinema.ac.id

**Abstract.** Federated identity is a prime solution to deal with the challenge of identity management and access in digital era, ensuring the college student are able to access educational resources easily and securely. Federated identity enabling student to use one set of identity for many platforms such as academic information system, e-library etc. Hence, it helps reducing the security risk such as password fatigue and password re-cycling to access them. The Technology Threat Avoidance Theory (TTAT) was implemented in this study to assess what variables motivate users to apply a federated identification system. Structural Equation Modelling was used for analyzing data, and the results suggested that the factors guiding users to apply a federated identification system were perceived threat, safeguard effectiveness, and self-efficacy.

# INTRODUCTION

In today’s digital era, college students harness many platforms and online services to support their academic activity such as learning portal, digital library, collaboration tool and research activity as discussed in [1-3]. However, utilizing various system often need a separated login mechanism with different credential, which can trigger password fatigue and potential security risk. Federated identity is a solution to encounter this issue, by giving student a space to utilize one credential set to access various system. By harnessing federated identity, it will increase user’s experience with an easy and consistent navigation system. By only having to remember one password, the risk of weak password usage or password re-cycling in various system can be minimized, hence it can gain the security in holistic way. Furthermore, this identity management has several advantages, including a better user experience, less administrative work, and higher security [4].

However, federated identity comes with some difficulties and dangers, particularly in security and privacy. Data breaches and unauthorized access are possible since multiple systems share users' identifying information. Exchanging personal data between organizations can raise legal and compliance concerns. In order to ensure that identity information is transferred safely with the right parties, [5] observed that "federated identity management must be able to tackle problems regarding security, privacy, and compliance”. A federated identification system that is applied by numerous universities and research institutions suffered a security incident in 2019 [6]. The breach is disturbing since it exposes the vulnerabilities of federated identification systems and the potential implications of a single point of failure. According to [7], those attacks on credentials emphasize the need of authentication mechanism and multiple factor authentication in federated identity management, to reduce the risk. All in all, though federated identity provides many benefits in terms of simplifying authentication and reducing administrative burden, it is necessary for university organizations to comprehensively assess the potential threats and to establish proper safety measures to minimize these risks.

Based on the description above, this study aims to determine what factors influence users continue to use federated identity on their accounts despite the many risks that can occur using Technology Threat Avoidance Theory (TTAT).

This paper is structured as follows: The literature review and the hypotheses are outlined in Section 2. The results of empirical test are presented in Section 3 and a comprehensive discussion of the results is presented in Section 4. Section 5 presents the conclusion.

# LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

## Technology Threat Avoidance Theory (TTAT)

TTAT is referred to as a theoretical framework that attempts to explore the factors which affect a decision made by an individual to accept or object a new technology. TTAT proposes that individuals tend to assess new technologies rely on their perceived susceptibility to risks and their perceived capability to encounter those threats. People tend to avoid using a certain kind of technology should they feel they are highly vulnerable and have limited ability to encounter those risks. People tend to utilize the technology, meanwhile, should they believe they are not particularly vulnerable and have a strong ability to deal with risks [8]. Eight factors are found in the TTAT, namely: Perceived Severity, Perceived Susceptibility, Perceived Threat, Safeguard Effectiveness, Safeguard Cost, Self-Efficacy, Avoidance Motivation and Avoidance Behaviour.

Avoidance behaviour depicts how an individual determine to avert or object new technology since how they believe it may produce risks [8]. With regards to TTAT, people will be more likely to get involved in avoidance behaviour should they feel there are serious upcoming risks associated with a technology and that it is predicted that there are unaffordable or preventive actions or inefficient precautions. Conversely, individuals are more inclined to employ the technology should they recognize that the risks are prohibited or effortlessly manageable and that the safety preventive actions are efficient and affordable. This theory has been triangulated by [9] in the context of spyware, and also [10] who further implements this theory.

## Hypotheses Development

Regarding to the TTAT, personal perception of threat is considered to be an important factor whether they are willing to accept or object a new technology [11]. The perceived severity of any potential hazards in the context of the technology is one of various constructs that have an effect on perceived threat. An individual tends keep technology in mind as threatening and recognize the possible hazards to be severe [12]. Therefore, with regards to the review mentioned above, the hypothesis can be drawn are as follow:

*H1: Perceived severity has an effect towards perceived threat*

The perceived susceptibility of an individual to likely risks in terms of the technology is one of numerous factors that influence the perceived threat. An individual tends to consider technology to be frightening and avoid harnessing, and they are vulnerable to the possible hazards [12]. To illustrate, a study carried out by Hoffman [13] revealed that individuals who believed they were more vulnerable to addiction of social media were less likely to identify the danger caused and to take preventative actions. With regards to the review mentioned above, a hypothesis is proposed as follows:

*H2: Perceived susceptibility has an effect towards perceived threat*

The degree to which an individual feel obliged to prevent the likely risks triggered by technology can be defined as avoidance motivation. An individual was inclined to be motivated to avert technology as it is harmful. With regards to this matter, a research that was carried out by [14] explored the elements that affects consumers' adoption of mobile payment systems. This research discovered that perceived risk, which is connected to perceived threat, incline avoidance catalyst in a favourable way. In terms of the review mentioned above, it can be drawn hypothesis as follows:

*H3: Perceived threat has an effect towards avoidance motivation*

Regarding to the TTAT, avoidance motivation contributes a crucial role in influencing whether they adopt or object a new technology. The degree of an individual's determination to avert likely threats presented by technology is defined as avoidance motivation. Some previous studies concurred with the concept that safeguard effectiveness has a constructive effect on avoidance motivation. For instance, a research conducted by [15] investigates the variables which affect the consumers' adoption of smart home technology. The research revealed that the perceived efficacy of privacy safeguards had a positive effect on avoidance motivation, which in turn had a negative effect on adoption intention. With regards to the review mentioned above, it can be drawn hypothesis as follows:

*H4: Safeguard effectiveness has an effect towards avoidance motivation*

The effort both mentally and physically required for implementing a particular safeguard action, including the money, time, comprehension, and inconvenience, is defined as the safeguard cost. It indicates that individuals tend to conduct a safety measure with less money, time, and effort to adopt. To illustrate, a study carried out by [16] explored the factors influencing mobile banking acceptance in Zambia. The study revealed that the biggest challenge to the acceptance of mobile banking was the perception of the cost of applying security measures. According to the authors, minimizing the perceived cost of security precautions may increase adoption intention and avoidance desire. In line with these reasoning, the following hypotheses can be suggested as:

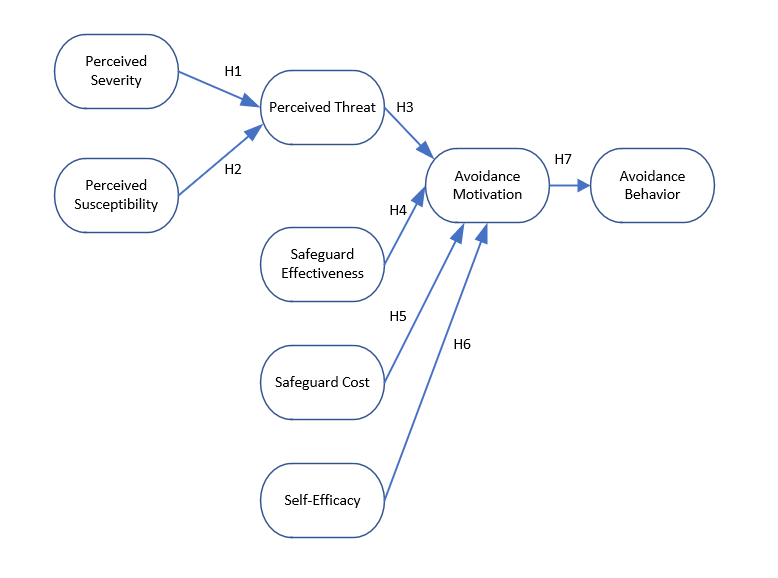
*H5: Safeguard cost has an effect towards avoidance motivation*

Self-efficacy concept illustrates an individual's trust in their ability to conduct a specific behaviour successfully. With regards to TTAT, an individual's choice to utilized a new technology is strongly affected by their sense of self-efficacy. Individuals are more inclined to adopt a technology as they are confidence in their ability to use it safely and successfully. In line with these reasoning, the following hypotheses can be presented as:

*H6: Self-efficacy has an effect towards avoidance motivation*

In terms of the TTAT, individual’s avoidance behaviour is examined by their avoidance motivation, the severity in which people recognize the threat triggered by new technology, how effective and expensive the available safeguards are, and how confident they are in their capacity to deal with it. Regarding to the hypothesis, people who observe a technology to be more dangerous tend to be motivated to avert it, and this avoidance motivate will probably cause in avoidance behaviour. In line with these reasoning, the following hypothesis can be suggested:

*H7: Avoidance motivation has an effect towards on avoidance behavior*

Research model of this study is displayed in Figure 1, which accommodates 7 aforementioned hypotheses.

**Figure 1.** Research model

# RESULT

## Measurement Development

A total of 300 respondents who were utilised as federated identity platform users submitted the data for the study. Data collected from a randomly selected group of college students using an interactive online questionnaire around 2021. Data has been examined in this study applying the Structural Equation Modelling (SEM) approach. SEM involves two phases, namely:

a. Confirmatory Factor Analysis (CFA) is used to confirm validity, i.e.: construct, convergent, discriminant, and composite reliability of the measurement model of all constructs.

b. For evaluating hypotheses to model and estimate the association between the constructs in the study, SEM is used.

## Confirmatory Factor Analysis (CFA)

The value of the Average Variance Extracted (AVE) can be used to evaluate CFA. The AVE value is reported to satisfy the requirements if it is more than 0.60. The main constructs and sub-constructs' AVE, which shows convergent validity, and Composite Reliability (CR), which measures reliability overall, are provided in Table 1.

**TABLE 1.** Average Variance Extracted and Correlation Matrix

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **AVE** | **CR** | **MSV** | **AVB** | **AVM** | **SEF** | **SC** | **SE** | **PT** | **PSUS** | **PS** |
| AVB | 0.885 | 0.955 | 0.112 | **0.722** |  |  |  |  |  |  |  |
| AVM | 0.791 | 0.873 | 0.381 | 0.435 | **0.845** |  |  |  |  |  |  |
| SEF | 0.622 | 0.811 | 0.212 | 0.345 | 0.332 | **0.722** |  |  |  |  |  |
| SC | 0.828 | 0.926 | 0.316 | 0.212 | 0.581 | 0.002 | **0.867** |  |  |  |  |
| SE | 0.732 | 0.813 | 0.278 | 0.376 | 0.221 | 0.113 | 0.207 | **0.642** |  |  |  |
| PT | 0.894 | 0.923 | 0.476 | 0.052 | 0.111 | 0.430 | 0.055 | 0.255 | **0.812** |  |  |
| PSUS | 0.843 | 0.907 | 0.413 | 0.803 | 0.013 | 0.103 | 0.228 | 0.467 | 0.344 | **0.789** |  |
| PS | 0.682 | 0.749 | 0.267 | 0.175 | 0.200 | 0.616 | 0.108 | -0.167 | 0.650 | 0.287 | **0.634** |

Construct validity was analyzed by model fitness index [17]. The results indicate a satisfactory fit for all three model fit categories [18]. The absolute fit index (RMSEA = 0.056) was met the expected level as it is less than 0.08, the incremental fit index of CFI = 0.962 and TLC = 0.636 was a good fit. The parsimonious fit index of chisq/df = 888.237 meet the expected level. Additionally, the TTAT model was significant at p-value=0.00. A good fitness index is expressed in a low Modified Index (MI) with MI less than 15 for each item [19], hence the data are exempted from multicollinearity issues. These model fit measurements need to be achieved before the data can be deemed eligible for further analysis.

## Structural Equation Modeling (SEM)

The results of hypothesis testing using path analysis can be seen in Table 2. Perceived threat was affected by perceived Severity (β=0.32; p-value=\*\*\*), whilst it was not influenced by Perceived Susceptibility (β=0.40; p-value=0.723). Perceived Threat itself is one of the constructs that influenced Avoidance Motivation (β=0.68; p-value=0.021), along with Safeguard Effectiveness (β=0.50; p-value=0.042), and Self Efficacy (β=0.12; p-value=\*\*\*), hence H3, H4, H6 were accepted. However, one construct was not significantly influenced Avoidance Motivation, that is Safeguard Cost (β=0.39; p-value=0.787), hence H5 was rejected. Lastly, this Avoidance Motivation affected Avoidance Motivation (β=0.44; p-value=0.038), therefore H7 was accepted.

**TABLE 2.** Structural Equation Modeling Result

|  |  |  |
| --- | --- | --- |
| **Construct** | **P-Value < 0.05** | **Result** |
| Perceived Severity 🡪 Perceived Threat | \*\*\* | Accepted |
| Perceived Susceptibility 🡪 Perceived Threat | 0.723 | Rejected |
| Perceived Threat 🡪 Avoidance Motivation | 0.021 | Accepted |
| Safeguard Effectiveness 🡪 Avoidance Motivation | 0.042 | Accepted |
| Safeguard Cost 🡪 Avoidance Motivation | 0.787 | Rejected |
| Self-Efficacy 🡪 Avoidance Motivation | \*\*\* | Accepted |
| Avoidance Motivation 🡪 Avoidance Behavior | 0.038 | Accepted |

# DISCUSSION

The objective of this study is to evaluate the variables that affect students’ intention to use the federated identity platform in a behavioral approach. There are 7 hypotheses tested in this study. Based on the hypotheses that have been tested, there are three variables that affect students’ use of the federated identity platform: Perceived Threat, Safeguard Effectiveness, Self-Efficacy toward Avoidance Motivation. Regarding to the Technology Threat Avoidance Theory, the empirical results of this study shows that Perceive Threat has an effect on Avoidance Motivation, because students who feel that their accounts are threatened either through data theft or unauthorized access will take preventive measures by utilizing federated identity. This is in accordance with the hypothesis that the greater the threat they feel, the greater their motivation to take action to avoid the threat. This is in line with research by [20]. Safeguard effectiveness affects avoidance motivation, which means that students feel that federated identity has advantages in maintaining the security of their accounts. By using federated identity, they feel that their accounts are protected by no longer using different accounts for each service provided, so that they can minimize password fatigue and password re-cycling. So, according to theory, the higher the students' trust in the reliability of the federated identity to protect them, the greater their motivation to avoid threats. This result supported study conducted by [21]. The next factor is Self-efficacy. Self-efficacy affects avoidance motivation shows that the more proficient students are in using federated identity, both understanding how it works and operating it, the more motivated they are that federated identity can help them avoid security threats to their accounts. This is in line with research by [22] which argued that self-efficacy has an effect toward avoidance motivation. For the next hypothesis, Avoidance Motivation influence Avoidance Bahaviour, the study reveals that people who are motivated to avert technology threats tend to adopt behaviours which is federated identity for the case. A study conducted by [23] support the result and argued that avoidance motivation was a paramount indicator of whether people were interested in taking security actions like setting up security software, avoiding from harmful online behaviour, and maintaining their systems updated.

With the use of this federated identity, students still feel the perceived threat, that their accounts are threatened by attacks, such as phishing or data breach. Perceived threat is affected by 2 factors, namely Perceived Severity and Perceived Susceptibility. Perceived Severity has an effect on Perceive Threat, which means that students feel that if their accounts are threatened, the impact will be great, for example their data will be lost or misuse of identity and data. This, in turn, enhances their likelihood of engaging in avoidance behaviors. The result of this study resembles with the results of research conducted by [24] which examined the variables affecting how likely consumers are to utilize mobile payment systems. However, this threat is not influenced by Perceived Susceptibility, which means that even though they know the magnitude of the threat to them, they feel that it will not happen to them. This is because they believe that the system provided by the university is guaranteed to be secure. That is what causes this hypothesis to have no effect. To illustrate, [25] examine in their study that perceived vulnerability had a negative ramification on the perceived threat linked with purchasing goods through online platform. Furthermore, this study’s result is confirmed with other hypotheses, namely safeguard costs that do not affect avoidance motivation. This is because students feel that federated identity has been provided by the university so that they feel they do not need to make an effort to use it nor cost any money. Similar to this, a study conducted by [26] investigated into the variables that influence consumers' aim for utilizing privacy-enhancing devices. With regards to the survey, a crucial challenge to the adoption of these technologies is the perception that use them will be unaffordable. Moreover, because there is no other choice of using federated identity, it will also not affect students’ decision not to use federated identity. In addition, if for example students are given the option whether they will use federated identity as a preventive measure, based on these results, they will not feel it as a threat, because they fully trust the university. The federated identity system provided by the university is seen by students as a means for the university to secure their accounts, so they believe that the university will make every effort to help secure their accounts from threats.

Based on these results, although students believe in the system provided by the university, there are impending risk. With this belief, students will become careless and ignore their safety condition. Therefore, it is essential to raise awareness in terms of security through digital literacy activities, especially in terms of data security. This will be studied further as the next issue to be addressed in this study.

# CONCLUSION

Federated identity in educational institution provide a good solution to address the challenge of advanced identity management. Federated identity facilitates educational institution in managing their resources and possible risks more effectively. Based on these results, although students understand the importance of using federated identity through hypotheses of Perceived Threat, Safeguard Effectiveness, Self-Efficacy toward Avoidance Motivation, there are impending risk, which is security awareness. Therefore, it is important to educate students in terms of security through digital literacy activities, especially in terms of data security and privacy.

# References

1. S. Affouneh, S. Salha, M. Agyemang Adarkwah, and A. Tlili, “A Large-Scale Study on the Preferred Learning Mode in Higher Education: Which One Suits Me Better in the New Normal?,” Int. J. Emerg. Technol. Learn. **19**(04), 4–16 (2024).
2. P. Toomnan, “The Impact of Online Learning during the COVID-19 Pandemic on Language Learning Strategies, Proficiency, and Enjoyment among Thai EFL Students,” Int. J. Emerg. Technol. Learn. **19**(01), 131–146 (2024).
3. H. Qin, Z. Shan, and Y. Du, “A Research into Factors that Influence College Students’ Enthusiasm for Learning in an Online Learning Environment,” Int. J. Emerg. Technol. Learn. **18**(18), 138–149 (2023).
4. A. Baldwin, M. Casassa Mont, Y. Beres, and S. Shiu, “Assurance for federated identity management,” JCS **18**(4), 541–572 (2010).
5. N. Kshetri, “1 Blockchain’s roles in meeting key supply chain management objectives,” International Journal of Information Management **39**, 80–89 (2018).
6. J. Li, W. Xiao, and C. Zhang, “Data security crisis in universities: identification of key factors affecting data breach incidents,” Humanit Soc Sci Commun **10**(1), 270 (2023).
7. J. Jensen, “Federated Identity Management Challenges,” in *2012 Seventh International Conference on Availability, Reliability and Security*, (2012), pp. 230–235.
8. A. Gillam, “Technology Threat Avoidance Factors As Predictors Of Risky Cybersecurity Behavior Within The Enterprise,” All-Inclusive List of Electronic Theses and Dissertations, (2019).
9. Trinity University, D. Young, D. Carpenter, Longwood University, A. McLeod, and Texas State University, “Malware Avoidance Motivations and Behaviors: A Technology Threat Avoidance Replication,” AIS TRR **2**, 1–17 (2016).
10. D. Carpenter, D.K. Young, P. Barrett, and A.J. McLeod, “Refining Technology Threat Avoidance Theory,” CAIS, 380–407 (2019).
11. University of Wisconsin, F. Zahedi, A. Abbasi, University of Virginia, Y. Chen, and Auburn University at Montgomery, “Fake-Website Detection Tools: Identifying Elements that Promote Individuals’ Use and Enhance Their Performance,” JAIS **16**(6), 448–484 (2015).
12. R.A. Alsharida, B.A.S. Al-rimy, M. Al-Emran, M.A. Al-Sharafi, and A. Zainal, “An Integrated SEM-ANN Approach to Evaluating Cybersecurity Behaviors in the Metaverse,” International Journal of Human–Computer Interaction, 1–20 (2025).
13. V. Hofmann, L.M. Schwayer, N.E. Stokburger‐Sauer, and A.T. Wanisch, “Consumers’ self‐construal : Measurement and relevance for social media communication success,” J of Consumer Behaviour **20**(4), 959–979 (2021).
14. N.T. Ha, “The impact of perceived risk on consumers’ online shopping intention: An integration of TAM and TPB,” 10.5267/j.Msl, 2029–2036 (2020).
15. S. Nikou, “Factors driving the adoption of smart home technology: An empirical assessment,” Telematics and Informatics **45**, 101283 (2019).
16. L. Sakala, and J. Phiri, “Factors Affecting Adoption and Use of Mobile Banking Services in Zambia Based on TAM Model,” OJBM **07**(03), 1380–1394 (2019).
17. J.F. Hair, *Multivariate Data Analysis*, 8th ed. (Cengage Learning India, Delhi, 2023).
18. A.S. Shkeer, and Z. Awang, “Exploring the Items for Measuring the Marketing Information System Construct: An Exploratory Factor Analysis,” International Review of Management and Marketing **9**(6), 87–97 (2019).
19. P.A. Paden, “Hierarchical Structure of Abilities: Factorial Validation of Higher Order Constructs in Thurstone’s Primary Mental Abilities,” Educational and Psychological Measurement **41**(3), 803–813 (1981).
20. M.P. Gagnon, E. Orruño, J. Asua, A.B. Abdeljelil, and J. Emparanza, “Using a Modified Technology Acceptance Model to Evaluate Healthcare Professionals’ Adoption of a New Telemonitoring System,” Telemedicine and E-Health **18**(1), 54–59 (2012).
21. J. Fan, M. Shao, Y. Li, and X. Huang, “Understanding users’ attitude toward mobile payment use: A comparative study between China and the USA,” IMDS **118**(3), 524–540 (2018).
22. H. Krasnova, N.F. Veltri, and O. Günther, “Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture: Intercultural Dynamics of Privacy Calculus,” Bus Inf Syst Eng **4**(3), 127–135 (2012).
23. Y. Kim, and S. Nam, “A Study on the Effects of Individual Factors, Job Factors, and Organizational Factors on the Response Behaviors(EVLN) of Disaster Safety Management Officials in Local Governments,” Jkps **20**(3), 21–42 (2020).
24. İ. Daştan, and C. Gürler, “Factors Affecting the Adoption of Mobile Payment Systems: An Empirical Analysis,” Emaj **6**(1), 17–24 (2016).
25. C.-M. Chiu, M.-H. Hsu, and E.T.G. Wang, “Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories,” Decision Support Systems **42**(3), 1872–1888 (2006).
26. I. Bashir, and C. Madhavaiah, “Trust, Social Influence, Self‐Efficacy, Perceived Risk and Internet Banking Acceptance: An Extension of Technology Acceptance Model in Indian Context,” Metamorphosis: A Journal of Management Research **14**(1), 25–38 (2015).