USER'S ACCEPTANCE OF BIOMETRIC AUTHENTICATION SYSTEM

Salsabila Dona Sunandi and Deddy Priatmodjo Koesrindartoto
School of Business and Management, Institut Teknologi Bandung, Indonesia
Email: salsabila.dona@sbm.itb.ac.id

Abstract. The rising of document fraud and identity theft, alongside with new threats such as cybercrime has led to the understandable changes in a global scale which requires a new technological solution to be implemented. Biometric authentication comes as a solution, which refers as the application of computational methods to biological features, especially with regard to the study of unique biological characteristics of human (Hopkins, 1999). It has successfully established itself as a relevant manner to identify and authenticate individuals in a reliable and fast way, by using individual's unique biological characteristics. The use of biometric systems for personal authentication is a response to the rising issue of authentication and security. This paper aims to determine the factors that influence the. user's acceptance of using biometric authentication system that involves university students in Indonesia. To examine the user's acceptance of using biometric authentication system, this paper integrates the advanced version of Technology Acceptance Model (TAM) and analyze the data using Statistical Package for Social Science (SPSS) to 1000 university students in Indonesia. The results indicate that all factors are significantly affecting the user's acceptance of using biometric authentication system as a better securuity measure to customers unless one variable notably social influence.

Keywords: Biometric Authentication Sytem; Biometrics; Security; User's Acceptance; Technology Acceptance Model

INTRODUCTION

In 2013, Target affirmed Friday that debit card PIN information was stolen in its ongoing monstrous rupture, turning around its prior position that the codes were not part of the hack (Goldman, 2013). Several years afterwards, Verizon reported that the in 2017, information on millions Verizon accounts was exposed on an unsecured server (Pachal, 2017). It did not stop there; it continued with the massive breach that occurred in Canva. Reportedly, a hacker successfully stole its 139 million of its users (Cimpanu, 2019). The aforementioned accidents are merely a few of security breaches. Alongside the increase of use of IT technology and the need to protect data, it requires users to possess multiple accounts or passwords while it is easy to crack passwords, even for the strong ones (Marios, 2018).

Biometric authentication comes as a solution, which refers as the application of computational methods to biological features, especially with regard to the study of unique biological characteristics of human (Hopkins, 1999). Authentication can be defined as the process of confirming an identity claimed by an entity (Claus, 2018). There are few benefits can be accomplished from using biometric authentication in e-commerce systems, such as ease of use (since no data input (user ID and password) are required from the user) also reducing data vulnerability (Harby, Qahwajim, & Kamala, 2010).

Biometrics can be used to prevent identity theft and enhance security. Even though biometrics does not eradicate the possibility of a security breach, it helps to ensure the systems are difficult to compromise, which leads to ensuring the privacy of the information (Fulcher, 2004). Not only have biometrics become the convenient use to use, but many also perceive them to a safer way to access accounts. Information retrieved from Visa survey, 48% of the respondents believe biometrics are more secure than traditional passwords and PINs (Gemalto, 2018). Based on this model, a survey instrument will be developed and tested with Indonesian university students and those who already obtain Bachelor or Master or Doctor degree.

LITERATURE REVIEW

Biometrics

Biometric refers to “the application of computational methods to biological features, especially about the study of unique biological characteristics of human” (Hopkins, 1999). More generally, it is the measurable characteristics of individuals based on their physical features or behavioral patterns that can identify its users (Bennet, 2000). Its motivation is explicit to discover or affirm the character of people from inborn characteristics (UK Government, 2018). There lie two fundamental operating principles underlying the biometric systems, namely authentication, and identification. The objective of authentication is to determine if a particular person is who he or she claims to be, for instance, to cash a check. On the contrary, identification is determined to capture a person’s biometric information; for instance, a passenger’s identity must be compared with the templates stored in the database. Generally, authentication systems regularly need active participation by its user (Bourkhonine, 2005).

Fingerprint

A fingerprint mark is an impression left by the contact edges of a human finger. A grinding edge (epidermal edge) is a raised bit of the epidermis on the fingers and toes, the palm of the hand or the underside of the foot (Fingerprints, 2017).

Face ID

Face recognition is one of the most significant biometric, which is by all accounts a decent trade-off between fact and social gathering and parities security and security well. Likewise, it has an assortment of potential applications in data security, law requirement, and access controls (Tan X, Chen S., Zhou Z.-H., & Zhang F., 2007)

Technology Acceptance Model

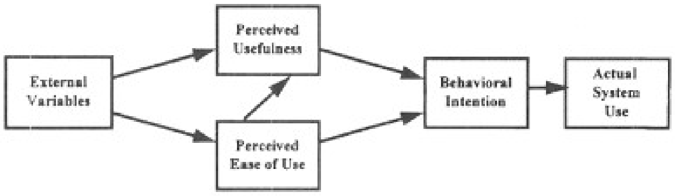

Figure 1. Technology Acceptance Model Framework

According to Fred D. Davis., P. Bagozzi and Paul R. Warshaw (1989) Technology Acceptance Model is an information systems theory that develops how users come to accept and use a technology. This framework was adopted by Theory Reasoned Action (TRA) created by Ajzen and Fishbein. TRA model is based from social psychology backgground and focusing on beliefs influence attitude effect, lead into intention then generate behavior (Fishbein and Ajzen, 1975). TAM suggests that when users are presented with a new technology, a number of factors influence their decision about how and when they will use it, notably:

1. Perceived usefulness (PU): The degree to which a person believes that using a particular system would enhance his or her job performance (Davis et al., 1989).
2. Perceived ease-of-use (PEOU): The degree to which a person believes that using a particular system would be free from effort (Davis et al., 1989).

During the time, TAM has been adopted by various studies as the research model that has accommodated many factors transforming into extended another constructs. Therefore, this paper will construct the extended TAM to identify the user’s acceptance towards biometric authentication system. This paper extends the TAM model to account for the new product attributes and social influence that are not originally included in TAM model. These two variables are not completely enclosed to biometric authentication, but are also valid to be used to other technologies. (Mukherjee & Hoyer, 2001).

ISBN: 978-623-92201-0-5

METHODOLOGY

To collect the primary data, this paper will distribute an online questionnaire to gather demographic respondent and respondent data regarding the questionnaire structure that this paper constructs from each variable.The proposed model for this paper is extracted by Harby et al., where this model consists of Social Influence (SI), Behavioral Intention to Use (BI), Actual Sytem Use (A), Perceived Usefulness (U), Perceived Ease of Use (E) and New Product Attributes (NPA).

The research framework and the relevant hypotheses for user acceptance of biometrics authentication were mainly developed based on the intrinsic features of the TAM model. The research hypotheses are constructed from previous studies by Harby et. al (2010). Two other intrinsic factors were added, notably new product attributes and social influences. New product attributes on biometric system characteristics was introduced to the model that reflects the uncertainty currently associated with the online banking secure authentication Cheng et al., 2006). On the other hand, the introduction of social influence is known as a subjective norms in many theories. (Venkatesh et al., 2003). It acts as one of the determinants of behavioural intentions to accept the system.

Social Influence is referred as the degree to which an individual perceives that important others believe that he or she should use the new system (Venkatesh, Morries, Davis, & Davis, 2003). Kelman (Kelman HC, 1958) was intrigued to understand the changes that involved external inputs such as information retrieved for them. Behavioral intention is a subjective probability of users that will affect the behavior. The purposed of behavioral intention to use variable is to estimate the actual purchase and usage behavior of the user (Fishbein & Ajzen, 1975). This variable is aimed to mediate the affective result from perceived usefulness and perceived ease of use and later link into behavioral intention to use (Davis, 1989). Perceived Usefulness is defined as the degree to which users believe that using biometric authentication system would enhance security access (Davis, 1989). Davis (1989) also believes that a high in perceived usefulness will favor the relationship with the user's acceptance. Davis et al., (1989) define perceived of use as "the degree which a person believes that a particular system or product would be free from effort. Perceived ease of use is the major determinant of user's acceptance towards a particular technology (Schoultz & Slevin, 1975). New Product Attributes is determined to measure the extent to which the biometrics system characteristics could provide additional benefits and value to the process. This variable is aimed to measure the extent to which the biometric system characteristics can add value to the process (Mukherjee & Hoyer, 2001).

The hypotheses constructed are as below:

H1: The new product attributes of the biometric authentication system have a positive relationship with perceived usefulness.

H2: The new product attributes of the biometric authentication system have a positive relationship with perceived ease of use.

H3: The perceived usefulness of using the biometric authentication system will positively influence the attitudes towards using the technology.

H4: The perceived usefulness of using the biometric authentication system i will have a positive impact an individual's behavioral intention to use the technology.

H5: The perceived ease of use of the biometric authentication system will positively influence the perceived usefulness of using the technology.

H6: The perceived ease of use of the biometric authentication system will positively influence the perceived usefulness of using the technology.

H7: Perceived attitudes towards using the biometric authentication system will have a positive impact an individual's behavioral intention to use this technology.

H8: Social influence will positively influence the individual's behavioral intention to use the biometric authentication system.

FINDINGS AND ARGUMENTS

The online questionnaire that has been distributed show some overview, which consists of a set of 1000 subjects with an average age of 17 to 23 and 70% which are female. The entire community is aware of biometric technologies and 86.5% of the respondents have reportedly used the technology. This paper also incorporated digital savviness for the respondents. The questions measure the level of digital savviness which classified into six groups, namely expense, transportation, leisure, knowledge, communication and investment. Each group consists of three to four questions. Questions which has high association with the usage of internet mark higher score, ranging from 1 to 10. The result indicated that the total respondents' digital savviness mark for 2.7. It shows that people have integrated their life into more digitalized lifestyle ones.The tested model has proved its reliability with Cronbach's Alpha. Every item should be at least 0.7, for the item to be included. George & Mallery stated that every item should be at least 0.7. Else, the questionnaire passed the validity data, exceeds the minimum requirement which is 0.5 score of Kaiser-Meyer-Olkin to be valid (Cerny & Kaiser, 1977).

Path Analysis

Path analysis is a technique for analyzing the causal relationship that occurs in multiple regression if the independent variable affects the dependent variable not only directly but also indirectly (Retherford & Choe, 1993). Sarwono (2010) suggests path analysis technique is used to analyze the causal relationship inherent between variables arranged in a temporary sequence using path coefficients as the amount of value in determining the influence of exogenous independent variables on endogenous dependent variables.

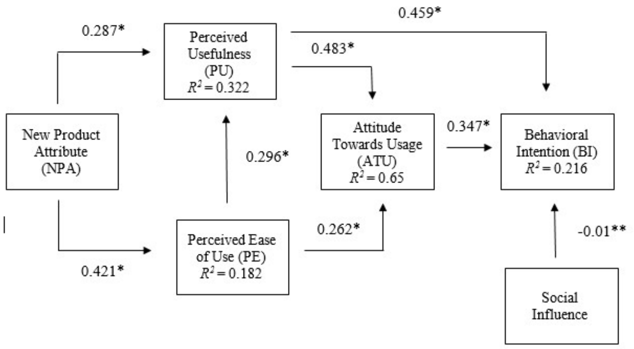
0.459*
0.287*
Perceived Usefulness (PU) $R^2 = 0.322$
0.483*
New Product Attribute (NPA)
0.296*
Attitude Towards Usage (ATU) $R^2 = 0.65$
0.347*
Behavioral Intention (BI) $R^2 = 0.216$
0.262*
-0.01**
Perceived Ease of Use (PE) $R^2 = 0.182$
0.421*
Social Influence

Figure 14. Path Analysis Result

Note: *p = 0.000, **p ≥ 0.05

Figure 2 illustrates the linear regression summary with the beta score (β) of the relationship of each variable. Some of the variables will get through the intervening variable before affecting the dependent variable.

Function 1

Based on Figure 4-1, the effect of perceived usefulness has a strong relationship towards the behavioral intention to use, as the path coefficient accounts for 0.459 (p < 0.05). The other path coefficients are the attitude towards usage, which accounts for 0.012 (p < 0.05). Social influence's p-value exceeds 0.05 with a beta score (β) of -0.01. It indicates that in Indonesia, social influence is not taken into account when it comes to adopting this technology, biometric authentication system. Conducting intense promotion through both online and offline channels or endorsing popular figure to encourage the usage of the system would not influence the decision of user's adoption. Ultimately, the data showed that social influence does not significantly affect the behavioral intention to use. These three paths acquire approximately 21.6% of the observed variance in the behavioral intention to use. Therefore, Hypotheses 4 and 7 are confirmed at the 0.05 level of significance, and Hypothesis 8 is not supported.

Function 2

The effect of perceived of usefulness and perceived ease of use have strong relationship towards attitudes towards using biometric authentication system. The perceived of usefulness has a path coefficient of 0.483 (p < 0.05). Meanwhile, the perceived ease of use is statistically significant (p < 0.05) at 0.262 of path coefficient. These three paths explain approximately 65% of the observed variance in attitude towards usage derived from these two paths. Based on this result, Hypothesis 3 and four are supported at the 0.05 significance level.

Function 3

Both new product attribute and the perceived ease of use are statistically significantly related to the perceived usefulness with a path coefficient of 0.287 and 0.296, respectively. The p-value of both is accounted for at p < 0.05. Thirty-two percent (32%) of the observed variance is required from these two paths. Therefore, Hypothesis 1 and six are confirmed at the 0.05 level of significance.

Function 4

Function 4 summarizes the relationship between new product attribute and the perceived ease of use. The data showed that both of these variables have a strong and significant relationship with 0.421 path coefficient (p < 0.05). This path clarifies 18.2% of the observed variance. Ultimately, Hypothesis 2 is supported with a 0.05 level of significance.

Another fact found in this study is that a new product attribute has strong a strong relationship with perceived ease of use. Additional characteristic such as biometrics authentication can be embedded into any form of devices, allowing people who have not adopted the technology will voluntarily attempt to use one. The new product attribute will influence the perceived ease of use of the system, but even if the system is already attached into a particular device but require much effort, people will be likely not to adopt one.

Possible causal chains can also be detected by using Path Analysis, namely:

a. Perceived Ease of Use → Perceived Usefulness → Behavioral Intention to Use
b. Perceived Ease of Use → Perceived Usefulness → Attitudes Towards Usage

Another fact to be unveiled is that social influence does not statistically significantly have a strong relationship with behavior intention to use. It does not determine whether someone would like to adopt a technology or not since their opinions cannot be comprised of any external inputs.

CONCLUSIONS

This paper has represented the user's acceptance of using biometric authentication system for Indonesian university students. The model developed in this study shown that the intention of the use of biometric authentication system is high. This paper used a quantitative method using online questionnaire based on Technology Acceptance Model (TAM) to evaluate user's acceptance of using biometric authentication system for Indonesian mobile phone user. This paper identifies a number of main factors influencing client behavioral intention towards using biometric authentication system. The results of testing model show that all factors significantly impact the adoption of this technology and signify that all of the seven hypotheses were confirmed unless for social influences. This implies that individuals believe in the benefits and the potential of this technology. Moreover, the bottom line of this research leads to the need of enhancing security of biometric technology.

REFERENCES

Bennet, P. (2000). Access control by audio-visual recognition in *Work Study* (pp. 23-26).

Boukhonine, S., V., K., & B., R. (2005). Future Security Approached and Biometrics. *Communications of the Association for Information Systems*, 937-966.

Cerny, C., & Kaiser, H. (1977). A study of a measure of sampling adequacy for factor analytic correlation matrices. *Multivariate Behavioral Research*, 43-47.

Cimpanu, C. (2019, May 24). *Australian unicorn Canva suffers a security breach*. Retrieved from ZD Net:

https://www.zdnet.com/article/australian-tech-unicorn-canva-suffers-security-breach/

Claus, K.-C. (2018). *How biometrics could finally replace PINs and passwords when we pay*. Retrieved from Ernst & Young: https://www.ey.com/en_gl/digital/how-biometrics-could-finally-replace-pins-and-passwords-when-we

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User. Acceptance of Information Technology. *MIS Quarterly, 13*, 319-339.

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research.* MA: Addison-Wesley.

Goldman, D. (2013, December 27). *Target confirms PIN data was stolen in the breach*. Retrieved from CNN Money: https://money.cnn.com/2013/12/27/technology/target-pin/

Fingerprints. (2017, July). *Biometric Technologies.* Retrieved from Fingerprints: https://www.fingerprints.com/asset/assets/downloads/fingerprints-biometric-technologies-whitepaper-2017-revb.pdf

Fulcher, J. (2004). The Use of Patient Biometrics in Accessing Electronic Health Records. *International Journal of Healthcare Technology Management*, 20-31.

Harby, F., Qahwajim, R., & Kamala, M. (2010). Towards an Understanding of User Acceptance to Use Biometrics Authentication Systems in E-Commerce. *International Journal of E-Business*, 34-55.

Hopkins, R. (1999). An introduction to biometrics and large scale civilian identification. *International Review of Law Computer and Technology*, 337-363.

Marios, S. (2018). *Introduction to Biometric and Applications.* Retrieved from ECE & CyLab, Carnegie Mellon University: https://users.ece.cmu.edu/~jzhu/class/18200/F06/L10A_Savvides_Biometrics.pdf

Mukherjee, A., & Hoyer, W. (2001, December 1). The Effect of Novel Attributes on Product Evaluation. *Journal of Consumer Research, 28*(3), 462-472.

Pachal, P. (2017, July 13). *If you're a Verizon customer, you should change your PIN — now*. Retrieved from Mashable: https://mashable.com/2017/07/13/verizon-data-breach/

Retherford, R. D., & Choe, M. (1993). *Statistical Models for Causal Analysis.* New York: John Wiley & Sons.

Sarwono, J. (2010). *Analisis Jalur Untuk Riset Bisnis dengan SPSS* (5 ed.). Yogyakarta: Andi.

Tan X, Chen S., Zhou Z.-H., & Zhang F. (2007). Biometric Security based on face recognition. *Pattern Recognition, 39*, 1725-1745.

UK Government. (2018). *Biometrics: a guide.* Retrieved from Government Office for Science: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715925/biometrics_final.pdf

Venkatesh, V., Morries, M., Davis, G., & Davis, F. (2003, September). User Acceptance of Information Technology: Toward A Unified View. *MIS Quarterly, 27*, 425-278.