"Do I Really Need to Use a Lock Screen?" : An Evaluation of Indonesian Smartphone Users

Ari Kusyanti
Department of Information Technology
Universitas Brawijaya
Malang, Indonesia
ari.kusyanti@ub.ac.id

Harin Puspa Ayu Catherina
Department of Information System
Universitas Brawijaya
Malang Indonesia
harinpuspa@gmail.com

***Abstract*—Nowadays, smartphone diversifies its functionality to store users' personal data including their sensitive information, which needs protection from unauthorized access. Lock screen is the simplest security method to guarantee the security of smartphone. This study aims to determine the factors that affect users in using lock screen as a lock on their smartphone by using 8 variables adapted from previous research. Data analysis used is Structural Equation Modelling (SEM) analysis. The results of this study suggest that the factors that influence users in using lock screen on their smartphone are trust, attitude and perceived risk.**

Keywords—lock screen, smartphone, user behavior, perceived security, trust, perceived privacy, perceived risk

I. INTRODUCTION

Smartphones as a means of communication are currently no longer used only for sending, receiving messages and placing phone calls, but also used to store users' personal data including their sensitive information. It's important for users to protect their smartphones from various threats that can result from unauthorized access to the system. Lock screen is the simplest smartphone's security method to guarantee the security of their smartphone and also the privacy of their data.

At present, the most commonly used authentication mechanisms on smartphones are slide or swipe, PIN, password, unlock pattern and biometric (e.g. fingerprint or face unlock). Because it is very often used, issues of security and usability are more important to note. The lock screen authentication system needs to be able to prevent unauthorized parties from easily gaining access to smartphone (security) devices. In addition, the system on lock screen authentication also needs to minimize user burden (usability), in terms of both cognitive load (e.g., remembering a PIN) and the time needed to successfully authenticate the PIN.

In the use of authentication mechanisms through PIN and unlock pattern, many smartphone users who consider using PINs become difficult, such as using passwords that are quite complicated and easily forgotten, besides that very few users change their PIN regularly for higher security [1] PIN and unlock pattern are both very vulnerable to guessing attacks from hackers. Because, generally users who use PIN and unlock patterns tend to use PINs and unlock patterns that are easy to remember and as a result, hackers can easily hack their PIN or unlock pattern [2].

In addition, the use of PIN and unlock pattern as lockscreen on smartphones is also very vulnerable to hackers who deliberately spy on input made by users to steal their PIN or unlock pattern [3]. In a study conducted by Aviv et al [4] found that stains found on smartphone screens can be easily used to find out unlock patterns on smartphones. In addition, attacks through the channel side use built-in sensors (e.g. accelerometer, microphone, etc.) have also been proven as an efficient way to hack PIN or unlock pattern from a user's smartphone. Another lockscreen is biometrics which aims to identify people who use unique features of physiological characteristics or human behavior such as fingerprints, sounds, faces, and irises [5]. This authentication method can naturally provide a very high level of security.

Based on the description above, this study aims to gain an understanding of the factors that affect smartphone users in using lock screen to protect smartphone security by Braber [8] entitled " Security and Privacy Perceptions of Millennials (18-24) and Non-Millennials (36-50) on Facebook" which aims to find out what factors influence the user's intention to use social media even though there are problems regarding security and privacy that might occur and Jansen [9] entitled "Studying Safe Online Banking Behavior: A Protection Motivation Theory Approach".

This paper is organized as follows. Section II describe an explanation related to the literature review of privacy, security, trust, perceived vulnerability, perceived severity, perceived risk, attitude, intention and develop the hypotheses and proposes the research model in the study. Section III explains data collection method and measurement development. Section IV provides the results of empirical tests and followed by a discussion in Section V. Finally, conclusions are drawn in Section VI.

II. THEORITICAL FRAMEWORK AND HYPOTHESES

This section will discuss the overview of perceived privacy, security, trust, perceived vulnerability, perceived severity, perceived risk, attitude, intention and develop the hypotheses tested and proposes the research model

A. Perceived Privacy

Privacy is a serious matter when users will perform activities in cyberspace [10]. Culnan [10] also argues that privacy concerns are also the reason why some people choose to reduce activity in cyberspace or choose not to engage in cyberspace activity and provide their personal information incorrectly in cyberspace. Currently, only a small percentage of people believe that they can control the personal information they have shared with the public or their personal information is used or even sold for business purposes [10].

In this study, privacy factors as proposed by Braber [8] will be adopted. Privacy is defined as the degree of individual's concerns regarding their ability to control the collection of personal information they have provided, as well as to control the use of personal data [11].

B. *Perceived Security*

Most recently, security issues are one of the important issues and should be considered when individual will provide their personal information publicly. Online users are increasingly finding that they are exposed to security risks during their online activities. Risks that can be caused by security issues include manipulation of personal information already provided or various types of fraud and misuse of personal information already provided [12].

In this study, security factors as proposed by [8] will be adopted. Security is defined the extent to which the user believes in a system used is secure so that it will not pose a risk as to the disadvantage of the user [8].

C. *Trust*

Trust has a very important role in doing activities on the virtual world, because the virtual world users do not see each other face to face. Therefore, trust is a very important thing when one decides to use a service to provide their personal information to the public space.

In this study, trust factors as proposed by Braber [8] will be adopted. Trust is defined as the degree to which an individual's willingness to be vulnerable to the actions of others [13].

D. *Perceived Vulnerability*

Perceived vulnerability is defined as the degree of vulnerability opportunities for a hazard [14]. An individual believes that only people with important information or people who feel annoyed by the presence of hackers are the ones who have to be concerned about computer risks [15]. In this study, perceived vulnerability factors as proposed by Jansen [9] will be adopted.

E. *Perceived Severity*

Perceived severity is used to measure an individual's judgment that a threat will occur. If an individual considers that the threat is not a severe threat, they will likely ignore the possibility of an online threat and there would be no change in behavioral intention [16]. Possible threats can also lead to exposure to important information and even personal data [17].

In this study, perceived severity factors as proposed by Jansen [9] will be adopted. Perceived severity is defined as the degree of the impact a user can perceive from a threat [9].

F. *Perceived Risk*

Risk is one factor that must be considered when using technology or an information system. An individual will tend to change their behavior based on how much risk they will receive for a particular threat [9]. The higher the perceived risk, will lead to the possibility that an individual will likely take protective measures [9]. The risks of privacy may also include misuse of personal information, such as the disclosure of personal identities or unauthorized access to such personal information.

In this study, perceived risk factors as proposed by Jansen [9] will be adopted.

G. *Attitude*

Attitudes are used to measure the extent to which users will continue to provide their personal information online in the future even if the user has learned that the service provider or other users may be benefiting or harming the user.

In this study, attitude factors as proposed by Jansen [9] will be adopted. Attitude is defined as the degree of individual positive or negative evaluative effects about performing target behaviour [18].

H. *Intention*

In this study, attitude factors as proposed by Braber [8] will be adopted. Intention is defined as the degree to which an individual's willingness to perform a particular behavior is influenced by the individual's attitude and the usefulness of the system [19].

I. *Hypotheses Development*

Yenisey et al. [20] defines security as the level to measure the level of individual's belief in a particular security. Kim [21] shows that sense of security is largely determined by the user's sense of control in a particular application. In a study of security it was mentioned that security from a broader perspective that includes not only technical aspects, such as confidentiality and authentication but also trust [22]. For instance, if the user decides to use lock screen on their smartphone, there are potential security threats that may occur [16]. A hacker can get into a smartphone via the internet and then insert a code to steal data to break into a smartphone's security system. Therefore, the mechanism of authentication on lock screen in smartphones must have a high level of security so that users can have confidence in the systems. From this statement, the hypothesis can be drawn as follows:

H1: Perceived security has a significant effect on trust.

The concept of privacy is generally defined as the ability of individuals to control the circulation of personal information they have provided [11]. The degree to which an individual believes that an application for personal information they have provided and also protects their privacy will indirectly impact their trust [21]. In the context of biometric systems, privacy refers to access that can be provided to others who have no authority to use such access [16]. For example, when using lock screen on their smartphone, there is always the risk that another user who has no authority to access the data [16]. Therefore, the mechanism of the authentication system must be able to maintain the privacy so that users have confidence in the authentication system. If someone believes that their privacy is protected, they will indirectly believe in the application. Based on the statement, the hypothesis is drawn as follows:

H2: Perceived privacy has a significant effect on trust.

In human interaction, trust has always been an important factor [23]. In day-to-day interaction, trust is an important determinant of sharing information and establishing new relationships [24]. Braber [8] suggests that trust has an impact on the attitudes and intentions of an individual. The smaller the risk caused by the use of an authentication system as a lock screen, the greater the user's trust in the authentication system on the smartphone. It will also make more positive attitudes and judgments from users of system authentication [16]. Users expect an

authentication system on smartphones, especially when they decide to use system authentication as a lock screen on their smartphone is an easy-to-use system so users believe that using the system is the right thing and can improve the user's attitude and positive judgment. Based on the discussion the hypothesis can be drawn as the following:

H3: Trust has a significant effect on attitude.

In the use of an application, trust is an important determinant of providing information. The greater the trust of a user to an application the greater the interest of a user in using the application [8]. For example, users should believe that they can protect their smartphone by using lock screen as an attempt to authenticate. Users should also believe that the lock screen can protect the data they have used for authentication. The belief of such users to trust the system can come from the use of similar systems before and from seeing others using such systems. Therefore, users should have confidence in authentication systems that they can protect their smartphone by using lock screen. When users can trust the authentication system that the system can protect them, they will tend to continue using the system. According to the review above, it can be drawn hypothesis as follows:

H4: Trust has a significant effect on intention.

Theory of Reasoned Action (TRA) shows that the performance and behavior of an individual is determined by individual's behavioral intentions. The behavioral intention of an individual is determined by the attitude of the person [8]. In this study, if someone has a positive attitude in protecting their smartphone with lock screen benefits them then it will make individuals continue to intend to protect their smartphone. From this statement, the following hypothesis is developed:

H5: Attitude has a significant effect on intention.

Perceived risk is defined as the potential loss caused by the use of an application [9]. In the context of the mechanism of the authentication system, the use of a lock screen on a smartphone is one of the user authentication processes. When users decide to use lock screen on their smartphone, of course, that will pose a risk [25]. This also allows hackers to abuse fingerprint data. When there are risks perceived by individuals in using the application, the individual indirectly will change their behavior based on how much risk they will receive for certain threats [26]. The higher the risk that might occur, the greater the individual's intention to take protective measures [9]. According to the explanation, the hypothesis is shown as follows:

H6: Perceived risk has a significant effect on intention.

Perceived vulnerability is defined as an assessment of the individual over the possibility of possible threats that may occur [27]. An example of using an authentication system on a smartphone is using fingerprint. The main purpose of adding biometric protection layer to the system is to reduce the vulnerability to security threats [16]. For example, if using a fingerprint on the lock screen of a smartphone, the disadvantage of using the system that is currently happening is that the fingerprint system they use as a lock of the smartphone can be copied using the provided template. A hacker can pretend to be the original user by providing the template and then copy the fingerprint of the user during the fingerprint recording process [25]. In this study, it involves an individual's belief in how likely it is to risk when they use a fingerprint to lock their smartphones. Based on the statement, the hypothesis is drawn as follows:

H7: Perceived vulnerability has a significant effect on perceived risk.

Perceived severity is defined as the perceived impact of a threat to the severity that might occur from security concerns [27]. One use of the authentication system on the lock screen in a smartphone is using a biometric pattern. Currently, the biometric layer itself can be a new target and draw the attacker's attention to attack the currently protected system when using the fingerprint used as a lock on the smartphone. This of course will be able to cause a threat to users who apply the use of fingerprints as authentication. The threats caused will also pose risks such as the misuse of their fingerprint data by unauthorized parties. In this study, it involves how severe the consequences of the occurrence of threats and risks when an individual uses a fingerprint to lock their smartphone. Based on the foregone review, the following hypothesis is developed:

H8: Perceived severity has a significant effect on perceived risk.

Based on the explanation of the hypothesis described above, the research model used in this study can be seen in Fig. 1

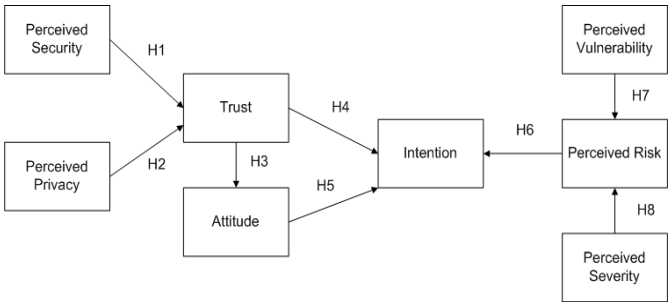

Fig. 1. Research Model

III. Methodology and Research Method

A. Measurement Development

These research constructs were measured using previously validated instruments. Perceived security, perceived privacy, trust, attitude and intention was measured using items adapted from Braber [8]. In the meantime, perceived vulnerability, perceived risk and perceived severity was measured using items adapted from Jansen [9]. The construct contained in this study was measured on a five-point Likert scale items, consists of 1: Strongly Disagree, 2: Disagree, 3: Neither Agree nor Disagree, 4: Agree, 5: Strongly Agree. The survey questionnaires are divided into two parts. In the first part, the participants had to provide demographic data, such as age, gender and background information related to lock screen usage. In the second part of the questionnaire, respondents were required to answer all questions in different constructs contained in the research model

B. Survey Design

The preliminary analysis is conducted using a pilot study that aims to validate the instrument, avoiding confusion when the respondent fill in the questionnaire and misinterpretation and to identify and detect errors and ambiguities. In this study, a pilot study was conducted by distributing questionnaires to 30 respondents. Then, the data obtained from the questionnaire was tested for reliability. To test the reliability of the data can be measured using the values of Cronbach's Alpha. If a variable has a Cronbach's Alpha value that is equal to or more than 0.6, it can be said that the variable is consistent and reliable [28]. In this study, all variables to be measured have been reliable.

IV. Data Analysis and Result

A. Mahalanobis Distance

This test is used to determine outlier data by using the value limit of the mahalanobis distance with an error rate of 1%. After searching for the mahalanobis distance value limit, the limit of the distance value of the mahalanobis distance is 44.314. Then, data that has a mahalanobis distance value of more than 44.314 must be eliminated and cannot be used in the subsequent analysis. In this study, out of 300 data there were 41 outlier data, so there were 259 data that could be used in the previous analysis.

B. Factor Analysis

This test is used to test the adequacy of the sample to be examined to determine whether factor analysis is appropriate for existing data samples [29]. To test the adequacy of data using Kaiser-Meyer-Olkin calculations. Based on the results of testing in this study obtained Kaiser-Meyer-Olkin value of 0.814, so it can be said that the adequacy of the data from the sample to be studied has criteria that are classified as great.

C. Normality Test

Normality testing is used to determine the distribution of data contained in this study has been normally distributed or not [29]. Data can be said to be normal if it has a significance value of more than 0.05. In this study, obtained a significance value of 0.075 so that it can be said that the distribution of data used has been normally distributed.

D. Homogenity Test

Homogeneity testing is used to determine the homogeneity of variance from the sample data to be used [28]. It can be said to be homogeneous if it has a significance of more than 0.05 [29]. Based on the results of testing that has been done, it can be seen that the variables used in this study have been homogeneous.

E. Measurement Model Fit

Measurement model fit is used to test and analyze the relationship of existing hypotheses between indicators and latent variables [28]. Testing fit measurement models can be done using Confirmatory Factor Analysis (CFA). The results of testing the fit model can be seen in Table II.

TABLE I. Measurement Model Fit Result

Index	Criteria	Value	Result
Chi-square ($\chi 2$)	$\chi 2$, df, p > 0.05	478.158	Good
Normed chi square ($\chi 2$/df)	< 5	1.962	Good
Goodness of Fit Index (GFI)	> 0.8 good fit	0.868	Good Fit
Root Mean Square Error of Approximation (RMSEA)	< 0.05 good fit	0.032	Good Fit

F. Structural Model Fit

Structural fit models are used to analyze the relationship between latent variables contained in the research model [28]. Structural model fit testing can be done using Path Analysis. The results of testing structural model fit can be seen in Table III.

TABLE II. Structural Model Fit Result

	Hypotheses	P < 0.05	Result
H1	Perceived Security → Trust	***	Accepted
H2	Perceived Privacy → Trust	0.004	Accepted
H3	Trust → Attitude	0.754	Rejected
H4	Trust → Intention	***	Accepted
H5	Attitude → Intention	0.022	Accepted
H6	Perceived Risk → Intention	***	Accepted
H7	Perceived Vulnerability → Perceived Risk	***	Accepted
H8	Perceived Severity → Perceived Risk	0.087	Rejected

Based on the results of testing the structural model fit that has been done, it can be seen that from the 8 hypotheses tested, there are 6 accepted hypotheses and 2 rejected hypotheses.

The impact of perceived security (P = ***) and perceived privacy (P = 0.004) on trust are significant at P = 0.05. Thus, H1 and H2 can be accepted. The impact of trust (P = ***), attitude (P = 0.022) and perceived risk (P = ***) on intention are significant at P = 0.05. Therefore, H4, H5 and H6 can be accepted. The impact of perceived vulnerability (P = ***) on perceived risk are significant at P = 0.05. Hence, H7 can be accepted. Meanwhile, it shows that perceived severity has no significant impact on the perceived risk, and accordingly H8 cannot be accepted.

Meanwhile, it shows that trust has no significant impact on the attitude. For this reason, H3 cannot be accepted.

V. Research Result and Discussion

A. Discussion on Hypothesis 1

Hypothesis 1 was accepted. Based on the results of hypothesis testing 1, it can be concluded that respondents have a high level of trust in security provided by smartphones when they decide to use lock screen on their smartphone so that they feel that there is a very low risk of data loss or access data by unauthorized parties. Respondents believe that when they use lock screen as a key on their smartphone it is safe and will not be manipulated by unauthorized parties. Respondents also believe that using lock screen on their smartphone is a trustworthy action because they believe that their smartphone vendors will protect their data safely and reliably. This shows this study of perceived security (PS) has a significant effect on trust (TR).

The results of this study are similar to the results of a study conducted by Braber [8] who suggested that when a service or technology has a high level of security and can protect data from its users, then these users will tend to have a high level of trust in the technology and feel that uses that technology.

B. Discussion on Hypothesis 2

Hypothesis 2 was accepted. Based on the results of hypothesis testing 2, it can be concluded that respondents believe when they decide to use the lock screen as a lock on their smartphone phone, they assume that their smartphone will guarantee their privacy by protecting the data used as their lock screen safely thus increasing the level of user confidence. In addition, respondents also assumed that lock screen is a trustworthy service provided by their smartphone vendors, because the services provided by the lock screen will be able to maintain the data contained in their smartphone safely and reliably to maintain privacy and security of users. Respondents thought that the vendor of the smartphone could be trusted and would not abuse the data lock screen they had used on their smartphone. This shows this study of perceived privacy (PP) has a significant effect on trust (TR).

The results of this study are similar to the results of a study conducted by Subramaniam et al. [30] who argued that when a service has a high value of privacy and can guarantee the privacy of user data it can be protected safely, it will make users have a high level of trust in the service.

C. Discussion on Hypothesis 3

Hypothesis 3 was rejected. Based on the results of hypothesis testing 3, it can be concluded that respondents believe that using a lock screen on their smartphone is something that can be trusted. In addition, for respondents giving information on their lock screen to their smartphone is a good idea. However, the trust in these smartphones that will not abuse the lock screen information that they have provided does not affect the attitude of users who will still provide information about the lock screen they use on their smartphones. This shows that in this study trust (TR) has no significant effect on attitude (AT).

The results of this study are the same as the results of research conducted by Barriere [31] suggesting that there is no influence between trust and attitude because the user's attitude in using a technology or service has no relation to the trust of the user.

D. Discussion on Hypothesis 4

Hypothesis 4 was accepted. Based on the results of hypothesis testing 4, it can be concluded that respondents assume that lock screen is a trustworthy service. The respondent felt confident that the lock screen would not misuse the personal information provided by the respondent. In addition, smartphone vendors from the smartphones they use will also be consistent and always honest in the use of information from the lock screen that has been provided so that it makes the respondents have the intention to continue using the lock screen on smartphones as often as possible in the future. This shows this study of trust (TR) has a significant effect on intention (IN).

The results of this study are similar to the results of a study conducted by Braber [8] who suggested that the greater the trust of a user in the use of an application, the greater the interest of the user to use the application.

E. Discussion on Hypothesis 5

Hypothesis 5 was accepted. Based on the results of hypothesis testing 5, it can be concluded that respondents assume that when they decide to use the lock screen as a lock from their smartphone it is a positive attitude that does not cause harm and can benefit them. In addition, respondents also assumed that using a lock screen on their smartphone is a positive step that can protect their smartphone from unauthorized parties who can access data from their smartphone. Therefore, this makes the respondents have the intention to continue to use the lock screen as a lock on their smartphone. This shows this study of attitude (AT) has a significant effect on intention (IN).

The results of this study are similar to the results of a study conducted by Ahmed et al [32] which suggested that when a user has a positive attitude towards an application, the user will tend to have the intention of continuing to use the application.

F. Discussion on Hypothesis 6

Hypothesis 6 was accepted. Based on the results of hypothetical testing 6, it can be concluded that respondents assumed that respondents did not see any threats or risks to privacy and the lock screen information they had provided on their smartphones. Respondents also felt that they were not afraid if something unpleasant happened to their smartphone. In addition, respondents also know the risks of providing information that they use as a lock screen on their smartphones so that they can minimize the risks themselves that may occur. Thus, this will make respondents have the intention to keep using the lock screen on their smartphones in the future because they have an understanding of the risks that will occur so they can minimize it themselves. This shows this study of perceived risk (PR) has a significant effect on intention (IN).

The results of this study are similar to the results of a study conducted by Lafraxo et al [33] which suggested that when users feel that an application has a low risk, they will continue to use the application without burden.

G. Discussion on Hypothesis 7

Hypothesis 7 was accepted. Based on the results of hypothesis testing 7, it can be concluded that respondents believed that when they decided to use the lock screen on their smartphone, they felt that it was not vulnerable to attacks by unauthorized parties who wanted to hack their smartphone. Respondents also assumed that the lock screen they used would not be easily guessed and obtained by hackers. In addition, respondents assumed that using the lock screen as a lock on their smartphone would not pose a threat and would not cause risks that might occur. This shows the study of perceived vulnerability (PV) has a significant effect on perceived risk (PR).

The results of this study are the same as the results of a study conducted by Jansen [9] which suggests that when users have known in advance about possible threats that might occur they will be able to consider the risks that might occur.

H. Discussion on Hypothesis 8

Hypothesis 8 was rejected. Based on the results of hypothesis testing 8, it can be concluded that respondents think the consequences of the lock screen they use on their smartphones will be guessed and hacked by unauthorized parties who want to hack their smartphones. Respondents also assumed that later there would be consequences of an attack from malware that would be used to hack the lock screen used by users on their smartphones. In addition,

respondents also assumed that the malware used to hack their lock screen would be able to find patterns from their lock screen and then access the smartphone from that user. However, this also makes users tend to ignore the risks that might occur. This shows this study of perceived severity (PS) has a significant effect on perceived risk (PR).

The results of this study are the same as the results of a study conducted by Jansen [9] which suggests that when users ignore threats that can occur when they use the application they will also ignore the risks that might occur.

VI. Conclusion

Based on the results of the research conducted, it can be seen that there are 3 factors that influence the user's intention in applying the lock screen on their smartphone, namely: trust, attitude and perceived risk. The respondent felt confident that the lock screen would not misuse the personal information provided by the respondent. Respondents also thought that using a lock screen on their smartphone was a positive step that could protect their smartphone from unauthorized parties who could access data from their smartphone. Respondents also know the risks of providing information that they use as a lock screen on their smartphones so that they can minimize the risks that may occur themselves.

Furthermore, the result of this study can raise users' security awareness in term of protecting their smarphone to prevent a lot of potential problems.

References

[1] Clarke, N. L., & Furnell, S. M. (2005). Authentication of users on mobile telephones–A survey of attitudes and practices. Computers & Security, 24(7), 519-527.

[2] Joseph Bonneau, Soren Preibusch, and Ross Anderson. ¨ 2012. A Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking PINs. In Financial Cryptography and Data Security, Angelos D. Keromytis (Ed.). Lecture Notes in Computer Science, Vol. 7397. Springer Berlin Heidelberg, 25–40

[3] Emanuel von Zezschwitz, Alexander De Luca, Philipp Janssen, and Heinrich Hussmann. 2015b. Easy to Draw, but Hard to Trace?: On the Observability of Grid-based (Un)Lock Patterns. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15). ACM, New York, NY, USA, 2339–2342

[4] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge Attacks on Smartphone Touch Screens. In Proceedings of the 4th USENIX Conference on Offensive Technologies (WOOT'10). USENIX Association, Berkeley, CA, USA, 1–7

[5] Wang, Shuo., et al., 2011. *Biometrics on Mobile Phone.* China : Tsinghua University.

[6] Market Insight. 2018. Smartphone face ID means more than 1 billion fewer fingerprint sensors will be shipped from 2017 to 2021. https://technology.ihs.com/599415/smartphone-face-id-means-more-than-1-billion-fewer-fingerprint-sensors-will-be-shipped-from-2017-to-2021

[7] Zhang, Yulong., et al., 2015. Fingerprints On Mobile Devices: Abusing and Leaking. [pdf] FireEye Labs. Available on: https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf

[8] Braber, S. V. D. 2016. Security and Privacy Perceptions of Millennials (18-24) and Non-Millennials (36-50) on Facebook. 7 th IBA Bachelor Thesis Conference

[9] Jansen, J., 2015. Studying Safe Online Banking Behaviour: A Protection Motivation Theory Approach. Netherlands: Univeristy of Netherlands.

[10] Culnan, Mary J., and Pamela K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. Organization Science, 10 (1) : 104-115

[11] Metzger, M., 2004. Privacy, trust, and disclosure: exploring barriers to electronic commerce. Journal of Computer-Mediated Communication 9 (4).

[12] J.E. Scott, "Measuring dimensions of perceived e-business risks," Information Systems and e-Business Management, vol. 2, 2004, pp. 31-55.

[13] Dwyer, C., 2007. Digital relationships in the MySpace generation: results from a qualitative study. In: Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS), Hawaii, 2007.

[14] Liang H, Xue Y. Understanding security behaviors in personal computer usage: a threat avoidance perspective. J As Inf Syst 2010.

[15] Weirich, D., and M. A. Sasse. 2001. Pretty good persuasion: A first step towards effective password security in the real world. Proceedings of the 2001 Workshop on New Security Paradigms, Cloudscrofl, NM, September 10–13.

[16] Ngugi, Benjamin., 2013. ModelingThe Impact of Biometric Security on Millenials' Protection Motivation. Boston: Suffolk University.

[17] Zhang, Lixuan and McDowell, William C. (2009) 'Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords', Journal of Internet Commerce, 8: 3, 180 — 197

[18] Ajzen, I., & Fishbein, M., 1975, Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research, 129-385, Addison-Wesley, Reading, MA.

[19] Venkatesh, V Moris, M.G., Davis, G.B., and Davis F.D., 2003, "User Acceptance of Information Technology: Toward a Unified View," MIS Querterly, Vol.27, No.3, September.

[20] Yenisey, M.M., Ozok, A.A., Salvendy, G., 2005. Perceived security determinants in ecommerce among Turkish University students. Behaviour and Information Technology 24 (4), 259–274.

[21] Kim, W., 2008. Applying the technology acceptance model and flow theory to Cyworld user behavior.CyberPsychologyandBehavior11 (3).

[22] Flavian, C., Guinaliu, M., 2006. Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. Industrial Management and Data Systems 106 (5), 601–620.

[23] McKnight et al., 2002. The Impact of Initial Consumer Trust on Intention to Transact with a Website: A Trusting Building Model

[24] Coppola, N. W., Rotter, N., Hiltz, S. R. 2004. Building Trust in Virtual Teams. IEEE TRANSACTIONS ON PROFESSIONAL COMMUNICATION, VOL. 47, NO. 2, JUNE 2004.

[25] Reid, P. (2004). Biometrics for Network Security. Upper Saddle River, NJ: Prentice Hall.

[26] Workman, M., Boomer, W. H., Straub, D. 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior 24 (2008) 2799–2816.

[27] Crossler, R.E. (2010), "Protection motivation theory: Understanding determinants to backing up personal data", Proceedings of the 43rd Hawaii International Conference on System Science, pp 1-10

[28] Hair Joseph F, Jr., Black William C., dan Babin Barry J., Anderson Rolph E. & Tatham Ronald L., 2010. Multivariate Data Analysis, Seventh Edition. Pearson Prentice Hall, Pearson Education,Inc: New Jersey

[29] Field, A., 2009. Discovering statistics using spss. 3rd ed. [e-book]. Sage Publications.

[30] Subramaniam, B., and Andrew, A. 2016. Security and Privacy Perception on Online Brand Trust in E-Commerce Industry. Journal for Studies in Management and Planning.

[31] Barriere, J. M., 2016. The Influence of Trust on Attitude of Employees towards HR Analytics in Organisations. University of Twent.

[32] Ahmed, A., and Sathish, A. S. 2017. Determinants of Behavioral intention, Use Behaviour and Addiction towards Social Network Games among Indian College Students. Man in India 97(4):21-42

[33] Lafraxo, Y., Hadri, F., Amhal, H., and Rossafi, A. 2018. The Effect of Trust, Perceived Risk and Security on the Adoption of Mobile Banking in Morocco. Proceedings of the 20th International Conference on Enterprise Information Systems (ICEIS 2018) - Volume 2, pages 497-502.