Acceptance of Biometric Authentication Security Technology on Mobile Devices

William Ratjeana Malatji, Tranos Zuva, and Rene Van Eck

Abstract The development of mobile devices is quick and changes our daily personal and business lives. Every mobile user wants to be sure about individual data security, and for this reason, biometrics come into existence for mobile devices. Many studies were conducted on the acceptance of biometric authentication technology, but only a few of these studies focused on mobile devices-based biometry and the current study based on the mobile technology. To observe the reliability of the broadcast services, it is essential to offer better security for the biometry mobile phones. The limitations of this study were addressed by proposing a new mobile biometric technology acceptance model (MBTAM) that contains perceived humanness (PH), perceived interactivity (PI), and perceived social presence (PSP). The combined model for this quantitative study was tested on 302 mobile users through the distribution of the survey questionnaire, and examined by using the statistical package for social science (SPS). The results indicate that only one variable of the proposed model is not supported, which calls for further research. Furthermore, the functional elements of the research model become more prominent on the customer's intention to practice the mobile biometric device than the social elements. The research contributes to academic by suggesting new constructs that join together MBTAM to evaluate the possibility of mobile users to accept biometric authentication technology.

Keywords Mobile biometric technology acceptance model (MBTAM) · Perceived humanness (PH) · Perceived interactivity (PI) · Perceived social presence (PSP) · Statistical package for social sciences (SPSS)

W. R. Malatji (✉) · T. Zuva · R. Van Eck
Department of ICT, Vaal University of Technology, Andries Potgieter Blvd, Johannesburg 1911, South Africa
e-mail: villywr@gmail.com

T. Zuva
e-mail: tranosz@vut.ac.za

R. Van Eck
e-mail: rene@vut.ac.za

V. Bindhu et al. (eds.), *International Conference on Communication, Computing and Electronics Systems*, Lecture Notes in Electrical Engineering 733,
https://doi.org/10.1007/978-981-33-4909-4_11

1 Introduction

In a technological era, mobile devices are most increasingly used for basic communications as well as a tool for managing individual issues and processing data obtained from anywhere at any time [1]. Over recent years, information access from mobile devices has become mainstream both in business and personal environments. The world is turning out to be more connected and every mobile user wants to be sure about individual data security [2].

Mobile device services assist as the base for business transactions but the traditional way of providing the security privileges is represented in terms of a mixture of alphanumeric and symbols. This ancestral process leads the users to avoid using mobile devices for reaching business data [3]. With the increase of its functionality including mobile banking, internet access, remote work, e-commerce, and entertainment, more confidential data is stored on these devices. For these reasons, biometrics comes in existence for mobiles [2].

To intensify the reliability of Wi-Fi services over mobile phones, a new trending and advanced technology have emerged that is biometric technology for mobile devices to promote the security levels [4]. Biometric technology refers to any technique that reliably uses measurable physiological or behavioral characteristics of distinguishing one individual from another [5].

Many studies were carried out on the acceptance of biometric devices and applications, users' attitudes towards such devices, and measurements of impact on performance. However, only a few of the studies focused on the factors that affect the acceptance of biometric devices [6]. Many studies have insisted on an investigation behind the biometric technology and stated the issues which are faced with user acceptance [7]. The acceptance of biometrics for other technologies still needs to be investigated deeply [8].

There were very few studies that measured the acceptance of biometric authentication technology on mobile devices. Therefore, this study efforts to regulate the reception of biometric corroborate technology on mobile devices.

The layout of the article is arranged in the following manner. Section 2 describes the related works of the proposed system. Section 3 denotes the significance of the study. Section 4 describes the methodology for the proposed system. Section 5 illustrates the results, and Sect. 6 reviews the discussions. Section 7 proposes the future scope of the research, and finally, Sect. 8 concludes the research work.

2 Literature Review

In literature, there have been many research studies on the acceptance of biometric devices and applications, users' attitudes towards such devices, and measurements of impact on performance. However, only a few of those studies focused on the factors that affect the acceptance of biometric devices [6]. Besides, each one of

those examinations analyzed the adequacy of biometric procedures, however, do not contemplate the purposes for such acceptability. According to [9], many studies discussed the acceptance of technology, and the studies focused on technical issues such as algorithms, accuracy performance, etc.

The survey was carried out with 1206 respondents with the age of 18 years and above to find out the level of the acceptance of biometric technology (specifically facial recognition) from the Australian public [10]. This was achieved by asking how acceptable they thought it was if this technology was to be used in certain circumstances. It was found that 95% of respondents supported that the security can be used by airport staff as a way of passenger identification on police watch-lists. A similar report suggested with accuracy 92% of respondents have confirmed the security procedures chosen by the police for identifying the culprits in the criminal cases are of the video footage gathered through the security cameras. Among the survey report, quarter of the respondents weighed that this technology is not preferable for acceptance. One part of the respondents was bothering about the reflections of social media across these technologies (for example, Twitter, Facebook, and so on). It was found that 50% of the respondents declared this was an unacceptable technology to be applied [11].

Researchers conducted a review predicted on the physiological and behavioral biometric methods for user acceptance [12]. Later observed that these methods are rated very feeble in general except for fingerprint, voice, and hand geometry. All the above-mentioned studies have not been conducted based on mobile biometric devices.

According to [13], few studies have been conducted on mobile biometric devices and the good including the bad side of such devices were also discussed. Research conducted on both the pros and cons of the particular technique where there is no clear idea stated for the factors affecting the usage of biometric authentication technologies through mobile devices. The outcome of these factors is affecting the workplace, education, government sectors, and so on. Due to this report, there exists a phenomenon of technology for user acceptance [13].

Investigators studied modern mobile supporters towards their PDAs [14]. The particular biometric strategies were presented as elective confirmation measures to make sure about their mobile phones and observed that respondents reflected all techniques positively. The impediment of the investigation made by Clarke et al., Deane et al. and Furnell et al. [14–16] was that there was no attempt to comprehend the level of association concerning the members for biometrics on phones.

A portion of the effective determinants of biometric has been analyzed by Giesing [17] assessed the issues projected by the user and the social factors of biometric discovery. This examination leads to the new technology development towards the acceptance model designed by Davis [18].

3 Significance of This Study

By identifying the user acceptance issues from the research question, this research will at point consider how to address such issues to escalate the user acceptance of mobile biometric technology based on security. New devices are coming with biometric authentication security technology; however, few studies have tested the user acceptance of such technology on mobile devices. This examination will emphatically supplement the clients' consciousness of the biometric security reformation on cell phones. The findings of this study will assist decision-makers to be aware of the issues that affect users' decisions to welcome and utilize a specific system so that they would be capable of considering them during the development stage. It is hoped that this research would be beneficial to future researchers by providing them with helpful information about biometric authentication technology on mobile devices and some of their research questions may be answered by this study.

4 Methodology

4.1 Participants of the Study

Participants for this study were South African citizens in Vanderbijlpark. Three hundred and five (305) questionnaires were distributed to the target population. Only 302 responses were returned out of 305. The results of the demographic characteristics of the respondents are shown in Table 1.

Table 1 Questionnaire, source, and number of items

Constructs	Number of items	Source-citations
Perceived Ease of Use (PEOU)	4	Emily, Johnson and Carmen (2019)
Perceived Usefulness (PU)	4	Emily, Johnson and Carmen (2019)
Subjective Social Norm (SSN)	4	Barbara, Belanger and Schaupa (2017)
Perceived Humanness (PH)	3	Lankton, Knight and Tripp (2015)
Perceived Interactivity (PI)	3	Gao, Rau and Salvendy (2009)
Perceived Social Presence (PSP)	3	Lankton, Knight and Tripp (2015)
Intention to Use	2	Weng, Yang, Ho and (2019)
Actual Use of Mobile biometric device (AUMBD)	3	Asiimwe and Orebro (2015)
Trust	4	Cheng, Sun, Bilgihan and Okumus (2019)
Reliability	1	Tuunainen, Pitkanen and Hovi (2009)

4.2 Research Instruments

In this quantitative study, a simple random sampling technique was used to choose the participants. The items of this study in the survey questionnaire were constructed from the review of the related works that is appropriate to the research model. A five-point Likert—scale type measurement from one "strongly agree" to five "strongly disagree" was used in this study. After developing the questionnaire, it has been circulated to 30 participants (10% of the sample size) to ensure good clarity of questions, good length of instruments, and content completeness. The questionnaire is further sub-divided into two parts namely the first section and second section. The former part includes the details of the question linked to internet usage, technology expertise, demographics, and awareness of internet scams. The latter part consists of enquires about the estimation of the value of mobile biometrics (appropriate use of varied biometrics). Table 1 shows the questionnaire, source, and number of items. The questionnaire of this study was created based on the research framework derived from Ho et al. [19] shown in Fig. 1.

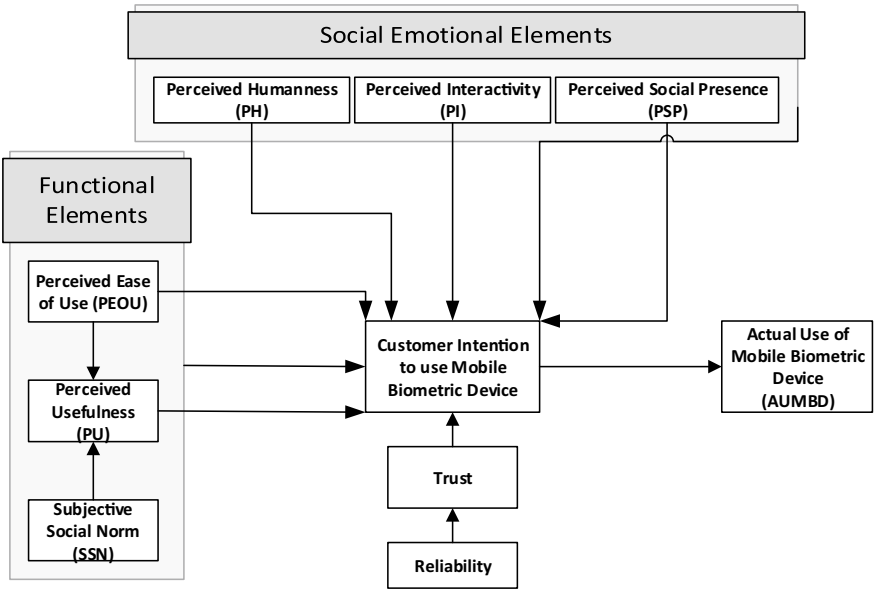

Fig. 1 Proposed mobile biometric technology acceptance model. *Source* Ho et al. [19]

5 Results

5.1 Demographic Characteristics

The data that is presented in Table 2 of this study provides the demographic characteristics of the respondents on age, gender, race, employment status, and the level of the study. The results indicated that 186 respondents were male and 116 were female, which shows that the number of male respondents is larger when compared to the number of female respondents. The greater number of the respondents is between 20 and 30 years of age with 69.9%, while the smallest is between 51 and 60 years of age with 2.3%. Considering the nature of mobile devices, this imbalance is understandable, because most mobile users are usually the youth [20]. Of the different races that participated in the study, the results indicated that 198 respondents were black, 87 were white, and 17 were other races. Regarding the participant's employment status, the results show that 8. 6% were self-employed, 25.5% were employed, and 1.0% retired, while 62.3% were students, and 2.6% other. It was further indicated in the results that on the level of the study, the majority of the respondents were undergraduate students with 38.7%, and the lowest was primary with only 3% (Tables 3, 4, 5 and 6).

5.2 Statistical Analysis

The displayed research model in Fig. 1 was evaluated by employing the statistical package for social sciences. The primary solution for factor analysis of this study revealed that the model was appropriate for factor analysis. The assumptions were tested, and it was found that the data contained no outliers, and the level of close to normality was excellent. The produced results indicated that the dependent variables do not violate the presupposition of linearity. Moreover, the results indicated that there is no presence of homoscedasticity and there is no multicollinearity. This shows that the statistical inferences made regarding the data may be reliable. In this study, items reliability test was performed and it was found that the reliability analysis of all variables was fairly high, which showed that the internal consistency among variables was robust and greater. Furthermore, items validity test was performed and the results indicated the satisfactory level of the construct validity of items.

5.3 Regression Analysis

The objective of this work is to measure user acceptance of biometric authentication technology on mobile devices, the analysis will focus on the main variables of acceptance in our acceptance model. The key variables of the customer's for the purpose

Table 2 Respondents demographic informations

Variable	Frequency	Percent (%)
Gender		
Male	186	61.6
Female	116	38.4
Age		
19 and Below	14	4.6
20–30	211	69.9
31–40	53	17.5
41–50	17	5.6
51–60	7	2.3
61 and Above	0	0
Race		
Black	198	65.6
White	87	28.8
Other	17	5.6
Employment status		
Self-employed	26	8.6
Employed	72	25.5
Retired	3	1.0
A student	188	62.3
Other	8	2.6
Level of study		
Primary	1	0.3
Secondary	11	3.6
Undergraduate	117	38.7
Postgraduate	97	32.1
Other	76	25.2
Do you own a mobile device		
Yes	294	97.4
No	3	1.0
Owned it before	5	1.7
Have you used biometric authentication security before		
Yes	215	71.2
No	87	28.8
Would you prefer to use a mobile biometric device		
Yes	256	84.8
No	15	5.0

(continued)

Table 2 (continued)

Variable	Frequency	Percent (%)
Not sure	31	10.3
I have accessed the internet using a mobile biometric device before		
Yes	141	46.7
No	161	53.3
Total	**302**	**100**

Table 3 Regression results of PU, PEOU, SSN, trust, PH, PI, PSP and intention to use

Model		Unstandardized coefficients		Standardized coefficients	*t*	Sig.
		B	Std. Error	Beta		
1	(Constant)	0.026	0.166		0.154	0.877
	PU	0.350	0.066	0.324	5.278	0.000
	POEU	0.195	0.063	0.162	3.054	0.011
	SSN	−0.054	0.038	−0.070	−1.418	0.157
	Trust	0.350	0.066	0.311	5.103	0.000
	PH	0.132	0.060	0.126	2.196	0.029
	PI	0.196	0.064	0.166	3.070	0.002
	PSP	0.211	0.052	0.229	4.030	0.000

[a]Dependent variable: intention to use

Table 4 Regression results of intention to use and AUMBD

Model		Unstandardized coefficients		Standardized coefficients	*t*	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.114	0.141		14.988	0.000
	Intention to use	0.224	0.072	0.177	3.107	0.002

[a]Dependent variable: actual use

Table 5 Regression results of PEOU, SSN, and PU

Model		Unstandardized coefficients		Standardized coefficients	*t*	Sig.
		B	Std. Error	Beta		
1	(Constant)	0.427	0.132		3.228	0.001
	POEU	0.589	0.048	0.576	12.340	0.000
	SSN	0.128	0.032	0.180	3.961	0.000

[a]Dependent variable: PU

Table 6 Regression results of reliability and trust

Model		Unstandardized coefficients		Standardized coefficients	*t*	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.207	0.182		6.634	0.000
	Reliability	0.466	0.052	0.468	8.971	0.000

[a]Dependent variable: trust

of using the mobile biometric devices (Intention to use) are PEOU ($\beta = 0.162$; $p < 0.05$), PU ($\beta = 0.324$; $p < 0.01$), PH ($\beta = 0.126$, $p < 0.05$), PI ($\beta = 0.166$; $p < 0.05$), PSP ($\beta = 0.229$; $p < 0.01$) and trust ($\beta = 0.311$; $p < 0.01$). The results indicate that trust and PU are the most important variables in explaining customer's intention to utilize the mobile biometric devices (Intention to use). Intention to use on its own is a key variable to AUMBD with ($\beta = 0.177$; $p < 0.05$). It is indicated in the results that PEOU is the most important variable that explains PU ($\beta = 0.576$; $p < 0.01$) succeeded by SSN ($\beta = 0.180$; $p < 0.01$). Moreover, reliability is the most important variable that explains trust with ($\beta = 0.468$; $p < 0.01$). The sum of functional elements of our model indicates that PEOU, PU, and SSN altogether, strongly explain intention to use with ($\beta = 0.390$; $p < 0.01$) (Fig. 2).

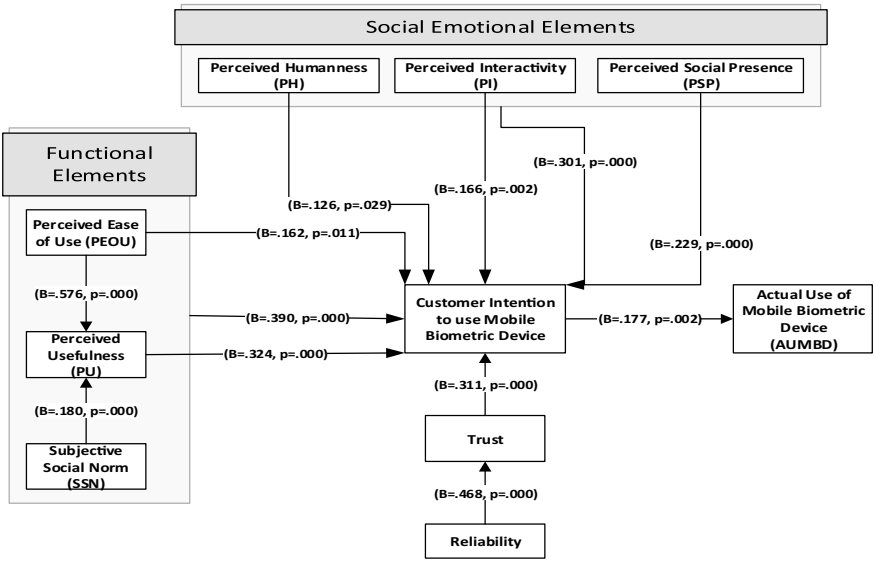

Fig. 2 Proposed Model for this study

6 Discussion

The overall mobile biometric acceptance model that is proposed in this study is validated. Starting with the functional elements (PEOU, PU, and SSN) of the model, the results indicated that PEOU has a positive influence on customers' intention to use mobile biometric devices (intention to use), and these results were supported by Suki and Suki [21]. This is an indication that when PEOU increases also intend to use increases. The results show that PU obtained impacts the positive plan to accept the usage of mobile, and these results are also in line with [21]. However, SSN on its own was not supported in this study. These same results were found on Chao [22]'s study on "factors determining the behavioral intention to use mobile learning: an application and extension of the ATAUT model." Based on the obtained results, it is concluded that PEOU and PU can be kept and used in future research to measure the acceptance of biometric authentication security technology on mobile devices. Although SSN is not supported, the variable on its own influence PU, moreover, the sum of all functional elements indicates a very strong influence on intention to use. Therefore, the conclusion cannot yet be made on whether the variable must be removed or not.

The social elements (PH, PI, and PSP) of the proposed model are all supported. It was indicated by the results that PI, PH, and PSP have a positive intention to use, and the results of these three variables are supported by Lankton [23]. Therefore, it is concluded that these variables can be kept and used in future research to estimate the user acceptance of biometric authentication technology on mobile devices [22]. Trust on its own is strongly influenced by reliability. Reliability is the most important variable that explains trust, and these results are in line with [7]. Intention to use on its own has a positive influence on AUMBD which is supported by Suki and Suki [21]. Based on these results, the conclusion can be made that trust, reliability, intention to use, and AUMBD can be kept and used in future research to measure the acceptance of biometric authentication technology on mobile devices.

7 Limitations and Suggestions for Further Research

This study focused on the two limitations as follows. Firstly, the study focused on the acceptance of biometric authentication technology on mobile devices only. Further research must be carried out on the acceptance of biometric authentication on other existing technologies except for mobile devices. The second important limitation of this study concerns gender and age of the respondents. The majority of the respondents for this study were male, and the highest age group of respondents was between 20 and 30. This brings about an issue of unbalanced results. Generally, both males and females in different age groups nowadays are using mobile devices. The conceptual framework used in this study should also be tested on the acceptance of biometric authentication technology on other existing technologies.

8 Conclusion

This study aimed to measure the acceptance of biometric authentication technology on mobile devices. The model that was used in this study proved to be valid, suitable, and supported. The researcher suggested that further research must be done especially using the variables that were supported in the model. The results and findings of this research showed that the majority of respondents acknowledged or are willing to accept biometric authentication technology to be used as security on mobile devices. However, further research needs to be conducted in this area.

Acknowledgements The author like to appreciate Professor Tranos Zuva and Doctor Rene Van Eck from the Vaal University of Technology for their support and supervision in this research. This is the revised version of the earlier paper. The author also likes to thank the IMITECH-2020's two anonymous reviewers for their valuable suggestions and comments throughout the research.

References

1. Wang H, Liu J (2009) Mobile phone-based health care technology. Recent Patents Biomed Eng 2(1):15–21
2. Kadena E, Ruiz L (2018) Adoption of biometrics in mobile devices. Obuda University, Doctoral school on safety and security sciences, Budapest Hungary. technologies to support teachers and improve practice
3. Bao P, Pierce J, Whittaker S, Zhai S (2011) Smartphone use by non-mobile business users. In: MobileHCI, Stockholm, Sweden. Attitudes and Practices: Computers & Security, vol 24, no 7, pp 519–527
4. Clarke N, Furnell S (2005) Authentication of users on mobile telephones
5. Kaur G, Kaur D (2013) Multimodal biometrics at feature level fusion using texture features. Int J Biometr Bioinform 7(1):58–73
6. James T, Pirim T, Boswell K, Reithel B, Barkhi R (2017) Determining the ıntention to use biometric devices: an application and extension of the technology acceptance model. J Organ End User Comput 18(3)
7. Chau A, Jamieson R (2004) Biometrics acceptance-perception of use of biometrics. Assoc Inform Syst
8. Uzoka FE, Ndzinge T (2009) Empirical analysis of biometric technology adoption and acceptance in Botswana. J Syst Softw 82:1550–1564
9. Chau A, Jamison R (2004) Biometric acceptance-perception of use of biometrics. In: ACIS 2004, Proceedings
10. Newspoll (2012) Rite aid deployed facial system in hundreds of Australia public. J Organ End User Comput 4(10):110–115
11. Unisys.Unisys security index report australia: facial recognition.https://www.unisyssecurityindex.com/system/resources/uploads/101/original/Australian2012.pdf
12. Miltgen L, Popovic C, Oliveira T (2013) Determinants of end-user acceptance of biometrics: ıntegrating the Big 3 of technology acceptance with privacy context. Decis Support Syst 56:103–114
13. Vrana R (2018) Acceptance of mobile technologies and m-learning in higher education learning: an explorative study at the faculty of humanities and social science at the University of Zagreb. Department for İnformation and Communication Science

14. Clarke NL, Furnell S, Rodwell PM, Reynolds PL (2002) Acceptance of authentication methods for mobile telephony devices 21(3):220–228
15. Deane F, Barrelle K, Henderson R, Mahar D (1995) Perceived acceptability of biometric security systems. Comput Secur 14(3):225–231
16. Furnell SM, Dowland PS, Illingworth HM, Reynolds PL (2000) Authentication and supervision: a survey of user attitudes. Comput Secur 19(6):529–539
17. Giesing I (2020) User perceptions related to ıdentification through biometrics within electronic business. University of Pretoria. https://upetd.up.ac.za/thesis/available/etd-01092004-141637/. Accessed 17 Feb 2020
18. Davis FD (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quart 13:319–339
19. Ho G, Stephens G, Jamieson R (2003) Biometric authentication adoption ıssues. In: Presented at the proceedings of the 14th Australasian conference on ınformation systems, Perth, Western Australia, 26–28th November 2003
20. Hosokawa R, Katsura T (2018) Association between mobile technology use and child adjustment in early elementary school age: Plos One J 13(7)
21. Suki NM, Suki NM (2011) Exploring the relationship between perceived usefulness, perceived ease of use, perceived enjoyment, attitude and subscribers' intention towards using 3G mobile services. J Inf Technol Manage (2011)
22. Chao C (2019) Factors determining the behavioural intention to use mobile learning: an application and extension of the UTAUT model. Front Psychol 10
23. Lankton M, McKnight DH, Tripp J (2015) Technology, humanness and trust: rethinking trust in technology. J Assoc İnform Syst 16(10) (2015)