FACTOR INFLUENCING CONSUMER INTENTION TO ADOPT BIOMETRIC AUTHENTICATION

IVY LU ZI YING

BACHELOR OF FINANCE (FINANCIAL TECHNOLOGY) WITH HONOURS

UNIVERSITY TUNKU ABDUL RAHMAN

FACULTY OF ACCOUNTANCY AND MANAGEMENT DEPARTMENT OF FINANCE

DECEMBER 2025

FACTOR INFLUENCING CONSUMER INTENTION TO ADOPT BIOMETRIC AUTHENTICATION

BY

IVY LU ZI YING

A research project submitted in partial fulfilment of the requirement for the degree of

BACHELOR OF FINANCE (FINANCIAL TECHNOLOGY) WITH HONOURS

UNIVERSITY TUNKU ABDUL RAHMAN

FACULTY OF ACCOUNTANCY AND MANAGEMENT DEPARTMENT OF FINANCE

DECEMBER 2025

Copyright @ 2025

ALL RIGHTS RESERVED. No part of this paper may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, graphic, electronic, mechanical, photocopying, recording, scanning, or otherwise, without the prior consent of the authors.

DECLARATION

We hereby declare that:

(1) This undergraduate research project is the end result of my own work and that due acknowledgement has been given in the references to ALL sources of information be they printed, electronic, or personal.

(2) No portion of this research project has been submitted in support of any application for any other degree or qualification of this or any other university, or other institutes of learning.

(3) The word count of this research report is _____.

Name of Student:	Student ID:	Signature:
IVY LU ZI YING	22UKB04262	*IVY LU ZI YING*

Date: 18/12/2025

ACKNOWLEDGEMENTS

I want to express my sincere gratitude to everyone who supported and guided me throughout this final year project.

Most importantly, I am deeply grateful to my supervisor, **Ms. Eaw Hooi Cheng**. Her unwavering encouragement and belief in my work were the true driving forces behind this project's completion. I am especially thankful for the way she shared her expertise; her constructive feedback and invaluable insights didn't just shape the scope of this research—they challenged me to think more deeply and grow as a student.

I also want to thank the University for providing the essential resources and facilities that made this work possible. Finally, my thanks go to the individuals who generously shared their knowledge and time to help me navigate the complexities of data collection.

TABLE OF CONTENTS

DECLARATION ..... **iv**

ACKNOWLEDGEMENTS ..... **v**

TABLE OF CONTENTS ..... **vi**

ABSTRACT ..... **x**

CHAPTER 1: RESEARCH OVERVIEW **1**

1.0 Research Background **1**

1.1 Background information **1**

1.1.1 Introduction of Biometric Authentication **1**

1.2 Problem Statement **6**

1.3 Research Questions **7**

1.3.1 General Question **7**

1.3.2 Specific Question **7**

1.4 Research Objectives **8**

1.4.1 General Objectives **8**

1.4.2 Specific Objectives **8**

1.5 Hypotheses of the Study **8**

1.5.1 Main Hypotheses: **9**

1.5.2 Control Variable Hypothesis **9**

1.6 Significance of the Study **9**

1.7 Conclusion **10**

CHAPTER 2: LITERATURE REVIEW **11**

2.0 Introduction **11**

2.1 Underlying Theories **11**

2.1.1 Technology Acceptance Model (TAM) **11**

2.2 Literature Review.....13

2.2.1 Perceived Usefulness (PU).....13

2.2.2 Perceived Ease of Use (PEOU).....14

2.2.3 Security and Privacy Risks (SPR).....15

2.2.4 Behavioural intention to adopt biometric authentication (BI).....16

2.2.5 Actual Usage Behavioural to adopt biometric authentication (AU).....17

2.3 Conceptual Framework.....19

2.4 Hypotheses Development.....20

2.4.1 Perceived Usefulness (PU).....20

2.4.2 Perceived Ease of Use (PEOU).....20

2.4.3 Security and Privacy Risks (SPR).....21

2.4.4 Behavioural intention to adopt biometric authentication (BI).....22

2.4.5 Control Variable.....22

2.5 Research Gap.....23

2.6 Conclusion.....25

CHAPTER 3: METHODOLOGY.....26

3.0 Introduction.....26

3.1 Research Design.....26

3.2 Data Collection Methods.....27

3.2.1 Primary Data.....27

3.3 Sampling Design.....28

3.3.1 Target Population.....28

3.3.2 Sample size.....29

3.3.3 Sampling Frame and Location 31

3.3.4 Sampling Technique 31

3.4 Research Instruments 32

3.4.1 Questionnaire Design.....32

3.4.2 Pilot Test 38

3.5 Constructs Measurement 40

3.5.1 Nominal Scale 40

3.5.2 Interval Scale 41

3.6 Data Processing 41

3.6.1 Data Checking.....41

3.6.2 Data Editing.....41

3.6.3 Data Coding 42

3.7 Data Analysis.....42

3.7.1 Inferential Analysis.....43

3.8 Conclusion 46

CHAPTER 4: DATA ANALYSIS 47

4.0 Introduction.....47

4.1 Descriptive Analysis 47

4.1.1 Usage of Biometric Authentication (Screening Question).....47

4.2 Inferential analyses 49

4.2.1 Measurement Model Assessment 49

4.2.2 Item reliability 49

4.2.3 Internal consistency reliability 49

4.2.4 Convergent validity 51

4.2.5 Discriminant Validity 51

4.2.6 Structural Model Assessment.....52

4.2.7 Predictive Model.....56

4.3 Bootstrapping Results by Age Group (Control Variable) 56

4.3.1 Young Age Group.....57

4.3.2 Middle Aged Group.....58

4.3.3 Older Aged Group.....58

4.3.4 Summary of Age-Based Differences.....59

4.4 Conclusion 59

CHAPTER 5: DISCUSSION, CONCLUSION, AND IMPLICATIONS.....61

5.0 Introduction.....61

5.1 Summary of Statistical Analysis 61

5.1.1 Summary of Descriptive Analysis 61

5.1.2 Summary Statistical Analysis.....62

5.2 Discussion on Major Findings.....63

5.2.1 Perceived Usefulness (PU) 63

5.2.2 Perceived Ease of Use (PEOU) 64

5.2.3 Security and Privacy Risks (SPR).....65

5.2.4 Behavioural Intention (BI) 66

5.2.5 Age as Control Variable 68

5.3 Implication of Study.....69

5.3.1 Theoretical Implications.....69

5.3.2 Practical Implications.....70

5.4 Limitations of the Study.....73

5.5 Recommendations for Future Research 74

5.6 Conclusion 75

REFERENCES.....**77**

APPENDICES.....**89**

ABSTRACT

As cybercrime and data breaches rise in Malaysia, many are questioning if traditional passwords and PINs are enough to keep them safe. While biometric authentication offers a more secure alternative, many Malaysians still hesitate to adopt it. This study explores why, using the **Technology Acceptance Model (TAM)** alongside **Security and Privacy Risks (SPR)** to understand the Malaysian consumer's mindset.

By analyzing 300 valid responses through **PLS-SEM**, the research found that while usefulness and security are important, the **ease of use** is actually the biggest factor driving people to switch to biometrics. The study also highlights that a person's intention to use the technology strongly predicts their actual daily usage. Interestingly, the data shows that age plays a significant role, with different generations approaching financial technology with varying levels of comfort. These insights provide a roadmap for Malaysian policymakers and developers to build more intuitive, trusted, and secure systems for everyone.

Keywords: Biometric Authentication, Technology Acceptance Model (TAM), Security and Privacy Risks, PLS-SEM, User Behavior, Malaysia, Cybercrime.

CHAPTER 1: RESEARCH OVERVIEW

1.0 Research Background

1.1 Background information

In recent years, the frequency of cyberattacks and data breaches has increased significantly worldwide. This happens because technology continue to evolve while cybercriminals are finding ways to take advantage of vulnerable online users. This led to people being concerned about global digital security. The growing number of security incidents also increases people's distrust in the effectiveness of traditional biometric authentication method such as passwords and Personal Identification Number (PINs). These methods are vulnerable to hacking, phishing, and data breaches which puts users' personal information at risk. In Malaysia, the cybersecurity situation has also faced serious challenges as there is a clear increase in cyber threats, data breaches and unauthorized leak of personal information. This heightened the need for consumer to adopt biometric authentication to protect themselves from cybercrimes.

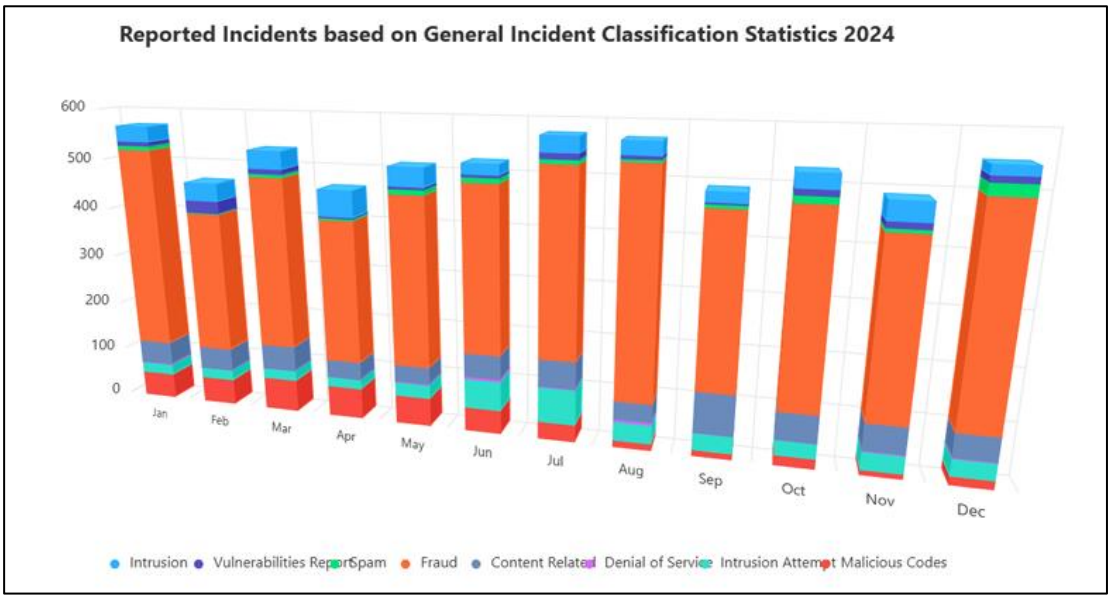
1.1.1 Introduction of Biometric Authentication

Digital world in today's, biometric authentication plays a significant role in ensuring cybersecurity for consumers. Biometric authentication refers to technologies that use unique physical characteristics (e.g., fingerprints, face recognition, iris scans) to verify identity. Before this technology such as passwords and PINs were used as the traditional authentication methods. Password was first introduced by computer scientist Fernando Corbató in 1961(Chatterjee, 2019; Zimmermann,2021) while PINs was developed in 1966 and implemented in

banking systems, and mobile access by 1967 (Maixé-Altés, 2021; Thodenius et al., 2011). Both methods were used back then because of their simplicity, ease of implementation, and low deployment cost. Despite their popularity back then, research have shown that they are not secure enough (Stylios et al., 2021). Besides, these methods also brought inconvenience to users due to the complexity of passwords combination. Although this approach enhanced the password strength (Zimmermann, 2021), but the complexity makes users difficult to remember. Research by Lovisotto et al. (2017) shows that 21% of users may forget their passwords within two weeks, and 25% forget at least one password every day, highlighting the impracticality of relying solely on passwords. In fact, in the digital word there are 51% of passwords are reused across services, and up to 80% can be cracked in less than three days, causing both security risks and usability burdens. This highlights the limitations of traditional password systems and explains why users prefer to reuse simple, indicating insecure credentials. Studies have also shown that PINs are no longer secure because most of the users select weak PINs, such as “1234” or their birth year, making them easy to guess (Markert et al., 2021). Due to their short length, PINs is vulnerable to brute-force attacks and shoulder surfing. Shoulder spying refers to an attacker directly observing a user's password input, thus obtaining the password without touching the device (Ku et al., 2016; Hirakawa et al., 2015; Binbeshr, 2022).

The increasing number of security threats has lowered users’ trust in digital security. For example, the "RockYou2024" data breach in 2024 exposed nearly 10 billion passwords, highlighting the widespread vulnerability of user credentials (Harris, 2024). Such a large-scale data breach has exacerbated concerns about the security of personal data, prompting users to question the reliability of traditional authentication methods. Additionally, the Bank Negara Malaysia's Annual Report 2020 states that cyber threats have continued to increase, with a total of 3,759 recorded in 2020, a 47% increase from the previous year (Moradi et al., 2022). Furthermore, MyCERT (2024) reported that in 2024, there were 4,219 fraud cases, 347 intrusions, and 97 spam incidents (Figure 1.1). These statistics prove that there is stronger needed a more secure authentication methods to overcome cybercrime.

Figure 1.1: MyCERT 2024 report



#	JAN	FEB	MAC	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Intrusion	29	34	34	49	36	19	29	25	17	26	33	16	347
Vulnerabilities Report	8	25	11	4	4	6	11	7	3	11	12	11	113
Spam	9	1	5	3	10	10	8	4	7	12	7	21	97
Fraud	401	282	342	284	337	326	365	441	333	372	334	402	4,219
Content Related	47	45	50	36	34	47	53	35	80	53	53	45	578
Denial of Service	2	0	0	0	2	5	2	5	1	0	1	2	20
Intrusion Attempt	21	22	22	20	27	59	69	37	34	30	34	33	408
Malicious Codes	50	51	64	61	56	46	34	13	10	18	9	15	427
	567	460	528	457	506	518	571	567	485	522	483	545	6,209

Adapted from: (MyCERT 2024 report)

Biometric authentication has become a highly advantageous and secure alternative to traditional authentication methods (Chaithra et al., 2025). This is because biometric authentication cannot be "reused" or "guessed". With It is unique and hard to duplicate by any other means. In addition, when using biometric features such as fingerprints and facial recognition, users do not need to enter any characters to complete the authentication, reducing the possibility of human error.

Figure 1.2: Evaluation of Users' account

TABLE 7: Evaluation of Users' accounts.

Security rating	Password (%)	Fingerprint (%)
Very secure	23.4	31.9

Source: (Moradi et al. 2022)

Figure 1.3: Fingerprint sensor authentication in IoT

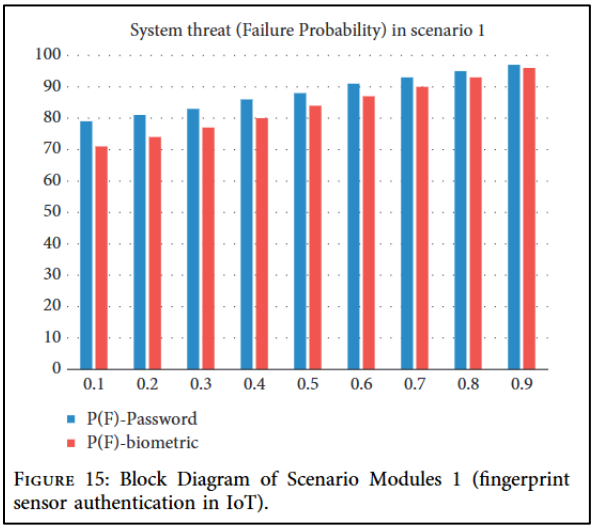


FIGURE 15: Block Diagram of Scenario Modules 1 (fingerprint sensor authentication in IoT).

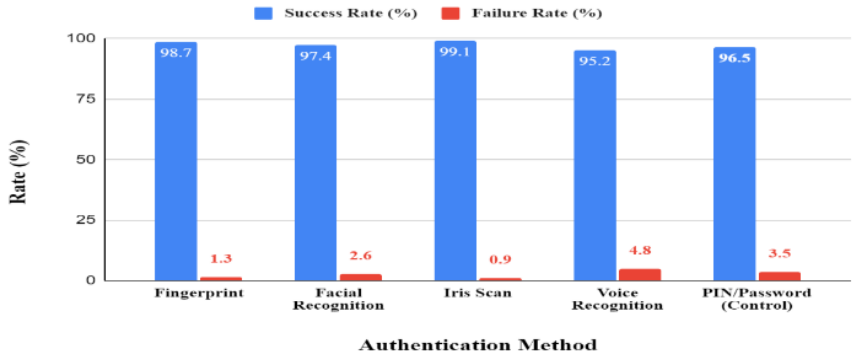
Source: (Moradi et al. 2022)

The research results shown in figure 1.2 and figure 1.3 show that biometric systems such as fingerprint recognition are more secure than traditional password-based methods. For example, the data in Figure 1.2 shows that users believe that fingerprint authentication is more secure than passwords. In addition, a study based on the Markov model shows that biometric fingerprint authentication can reduce the probability of a system being hacked by an average of 94.02%, highlighting its effectiveness in preventing security breaches (Moradi et al., 2022). In addition, the biometric authentication method used in the study has higher accuracy and is user friendlier than the PIN or password method.

Figure 1.4 Authentication Success Rate by Method

Table 1 Authentication Success Rate by Method

Authentication Method	Success Rate (%)	Failure Rate (%)
Fingerprint	98.7	1.3
Facial Recognition	97.4	2.6
Iris Scan	99.1	0.9
Voice Recognition	95.2	4.8
PIN/Password (Control)	96.5	3.5



Source: (Doddipatla et al., 2021)

Figure 1.5 Authentication Speed (Seconds) by Method

Table 2 Authentication Speed (Seconds) by Method

Authentication Method	Avg. Speed (Seconds)	Std. Deviation (Seconds)
Fingerprint	1.2	0.4
Facial Recognition	1.5	0.5
Iris Scan	1.6	0.3
Voice Recognition	2.4	0.7
PIN/Password (Control)	2.0	0.6

Source: (Doddipatla et al., 2021)

According to Figure 1.4 and 1.5, biometric authentication such as fingerprint and iris scanning outperforms traditional passwords and PIN codes in terms of success rate, authentication speed, and user satisfaction, especially in terms of success rate and authentication speed. For instance, Iris scan has a success rate of at least 2% higher than PINs or passwords while fingerprint has an authentication speed of 0.8 seconds higher than PINs or passwords (Doddipatla et al., 2021).

However, the main purpose of this study is to gain a deeper understanding of how perceived usefulness (PU), perceived ease of use (PEOU), and security and

privacy risks (SPR) can influence customers' willingness to use biometric authentication, and to explore how this willingness translates into actual usage behavior. Age acts as a control variable in this study to reduce demographic bias in the behavioral outcomes, as previous research has suggested that age influences technology adoption preferences.

1.2 Problem Statement

As shown above, with the rising number of data breaches and cyberattacks, strong security protection is indicated as needed. Studies show that traditional forms of security, such as passwords and personal identification numbers (PINs), cannot adequately safeguard sensitive data and customer details. Even with the passwords that have been provided, consumers' data and sensitive information remain open to serious breaches, hacking, and phishing attacks (Zhang et al., 2024). As a result, the cyber threat situation has getting worse.

To mitigate security risks, the use of biometric identification has been proposed. Identification methods such as fingerprinting, facial recognition, and iris recognition are some of the unique characteristics used to improve digital security (Khade et al., 2021). Although the great potential of security protection systems (biometric authentication) has not spurred its slow adoption. According to Nanda et al. (2024), when organizations do not impose the use of advanced forms of authentication, users do not voluntarily adopt them, which indicates that passwords are still the main form of authentication used. While biometric technology is available, the fact that it is not widely adopted suggests that potential users are not willing to embrace it. According to Elmir (2018), it shows the resistance stems from a lack of understanding and training regarding the potential advantages and capabilities of biometric technology, as well as concerns about privacy and security risks. Other users may not always achieve their desired results.

On the other hand, most current research on biometric authentication seems to focus primarily on the technical aspects, such as its advantages and disadvantages.

To bridge this gap, a deeper understanding of the key factors influencing consumer adoption or avoidance of such systems is needed. This study aims to examine determinants of parameters influencing willingness to use biometric authentication, such as perceived usefulness, perceived ease of use, and concerns about security and privacy. Age was used as a control variable to limit the impact of demographic bias. In addition, this will offer guidance to governments, FinTech companies, developers of biometric systems, and consumers about adopting strategies that stimulate and foster the wider use of biometric technologies to enhance global digital security.

1.3 Research Questions

1.3.1 General Question

This study proposes five research questions to explore factors influencing consumer acceptance of biometric technology, focusing on perceived usefulness, ease of use, and security and privacy risks. Identifying these factors will show which are significantly associated with consumers' actual acceptance behaviour. Age was used as a control variable to ensure impartial analysis. The specific questions are as follows:

1.3.2 Specific Question

[RQ1] What is the effect of Perceived Usefulness (PU) on consumers' behavioural intention to adopt biometric authentication?

[RQ2] How does Perceived Ease of Use (PEOU) influence consumers' behavioural intention to adopt biometric authentication?

[RQ3] What Security and Privacy Risks affect consumers' behavioural intention to adopt biometric authentication?

[RQ4] What is the relationship between consumers' behavioural intention and their actual use behaviour of biometric authentication?

[RQ5] How does controlling for age help ensure unbiased analysis of consumers' actual usage behavior of biometric authentication?

1.4 Research Objectives

1.4.1 General Objectives

To understand the reason for the consumers' behavioural intention (BI) in Malaysia, the primary purpose of this research is to determine the factors that affect actual use of biometric authentication.

1.4.2 Specific Objectives

[RO1] To identify the effect of Perceived Usefulness (PU) on consumers' behavioral intention to adopt biometric authentication.

[RO2] To investigate the effect of Perceived Ease of Use (PEOU) on consumers' behavioral intention to adopt biometric authentication.

[RO3] To evaluate the influence of Security and Privacy Risks (SPR) on consumers' behavioral intention to adopt biometric authentication.

[RO4] To evaluate the relationship between behavioral intention and actual use behavior of biometric authentication.

[RO5] To control for age in the analysis of actual usage behavior, ensuring that demographic differences do not bias the final behavioral outcomes.

1.5 Hypotheses of the Study

The Technology Acceptance Model (TAM) is the fundamental foundational theory for this research. To extend the security issues in TAM, this study includes security

and privacy risk (SPR) as an additional variable. Based on this study's, the following hypotheses are developed:

1.5.1 Main Hypotheses:

[H1] Perceived Usefulness (PU) has a significant influence effect on consumers' behavioral intention to adopt biometric authentication.

[H2] Perceived Ease of Use (PEOU) has a significant influence effect on consumers' behavioral intention to adopt biometric authentication.

[H3] Security and Privacy Risks (SPR) have a significant influence effect on consumers' behavioral intention to adopt biometric authentication.

[H4] Behavioral intention to adopt biometric authentication has a significant influence effect on actual usage behavior.

1.5.2 Control Variable Hypothesis

Age was used as a control variable to ensure that the observed effects were not affected by age.

1.6 Significance of the Study

The use of biometric authentication is growing as it becomes a part of many different digital services, which means that this study is very important from both a practical and an academic standpoint. This research aims to allow readers to learn about some of the influences on consumers when deciding whether or not to use biometric authentication. Moreover, it also helps bridge the gap between the technological innovation associated with biometrics and the acceptance of these technologies by users. By using established theories such as the Technology Acceptance Model (TAM) regarding how people adopt or use technology, the findings of this research provide insight into how companies can identify the needs of customers for increased use of biometric authentication technology as a means

of increasing the security of the digital finance sector. In addition, the findings of this research may encourage government agencies to consider and recommend the use of biometric systems in processes such as banking, medical care, and the creation of digital identities (Amini & Javidnejad, 2024).

1.7 Conclusion

In summary, this chapter discussed the research background, problem statement, research questions and objectives, and the significance of this study on the impact of biometric authentication on consumers.

CHAPTER 2: LITERATURE REVIEW

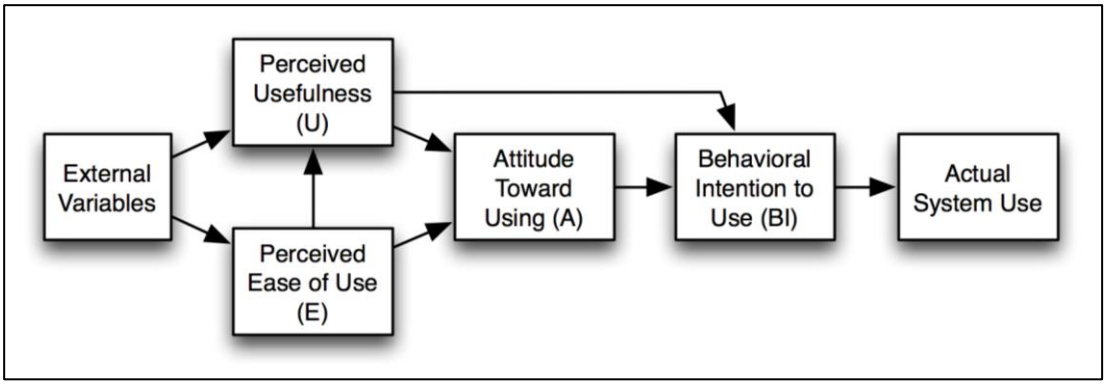
2.0 Introduction

This chapter discusses theoretical foundations, literature review, conceptual framework, hypothesis development, and the research gap of the study. The theory used as the guiding model in this study is the Technology Acceptance Model (TAM). The key variables examined in this study are perceived usefulness (PU) and perceived ease of use (PEOU), security and privacy risks (SPR), the intention to adopt biometric authentication (BI), and actual use behavior (AU). This chapter reviews prior studies and analyzes the relationships among these variables and proposes a conceptual framework.

2.1 Underlying Theories

2.1.1 Technology Acceptance Model (TAM)

Figure 2.1: Technology Adoption Model (TAM) Framework



Adapted from: (Davis, 1989)

The Technology Acceptance Model (TAM) was developed by Fred Davis in 1989 and has most widely used theories to explain technology adoption. It highlights how

users' perceptions characterize the acceptance of new systems and the related attributes of usefulness and ease of use (Saare et al., 2019). In this study, the Technology Acceptance Model (TAM) theory is utilized to examine the purpose of consumers' adoption of biometric authentication methods. This study uses TAM to examine how perceptions of biometric authentication affect users' willingness to adopt it as a secure digital solution.Across many categories, TAM has shown through research to consistently be an accurate predictor of new technology adoption through its many applications. As argued by Wang et al. (2021), adding the constructs of trust and privacy to the original model increases TAM's predictive power concerning the use of biometric authentication within FinTech. Similarly, Cheng (2018) also demonstrated that TAM can effectively explain changes in user acceptance under different conditions. These studies have illustrated the adaptability of the TAM, thereby justifying its employment as a theory to assess the adoption of biometric authentication in the current study.

According to the model from TAM, PU and PEOU are the major determinants of BI and hence technology acceptance (Davis et al., 1989). Based on Figure 2.0, technology acceptance takes three steps. First, users of any technology are influenced by external factors such as system design and user experience and can change a user's perception of the system to think they are PEOU and PU. Second, the perceptions of the system shape the user's attitude and intention. PEOU not only affects intention directly but also potentiates PU, as users find technology to be beneficial (Davis, 1989). Third, the model explains the relationship between perception, attitude, and consequent behavior. Perceiving a system as PEOU and PU towards technology, a user's attitude is positively biased, and hence their BI is increased (Davis, 1993). PU also significantly and directly affects BI, which is the strongest predictor of AU (Davis, 1993). In short, people who think technology is easy and beneficial will adopt it.

Within the context of the TAM, there are two important variables, such as PEOU and PU, that seek to explain why users adopt new technologies. PU is the degree to which an individual feels that using that technology will result in an improved or more effective outcome (Davis, 1989). Within biometric authentication,

PU is concerned with whether users feel that fingerprint or face recognition is a more secure and convenient method than traditional methods.For instance, the BioTAM framework integrated PU showed positive effect on users' behavioral intentions toward biometric systems (Kanak & Sogukpinar, 2017).

Additionally, PEOU means how much a person thinks using the system will be easy (Davis, 1989). Research shows that PEOU can enhance PU, because systems that are easier to use are often perceived as more useful (Davis, 1989). Moreover, PEOU include self-efficacy, which refers to users' confidence in using technology (Bandura, 1982) and perceived complexity mean how difficult the system is perceived to be (Peres et al., 2010). Both factors will affect the PEOU. Similarly, Dhagarra et al. (2020) highlighted that consumers are more likely to adopt technology that they believe are simple and convenient to use. Therefore, PU and PEOU are recognized as core cognitive foundations of TAM and remain widely validated (Davis, 1993; Hung & Chang, 2005).

In summary, the TAM provides a core framework that links PEOU and PU with attitudes, BI, and AU regarding biometric authentication, and is extended in this study by incorporating Security and Privacy Risks (SPR) as an additional contextual factor to better capture security-related adoption concerns.

2.2 Literature Review

2.2.1 Perceived Usefulness (PU)

Perceived usefulness (PU) is the degree to which an individual believes using technology will improve task performance or daily activities. (Davis, 1989). Within the TAM, PU is viewed as one of the most important variables influencing individuals' decisions to use new technology. (Venkatesh et al., 2003).

Regarding biometric authentication, a previous study had evidence to show a consistent positive impact of PU on BI. Stylios et al. (2022) studied the adoption

of European National Biometrics (BBCA) and found that individuals who believe biometrics is beneficial for protecting personal information and assisting daily activities are more likely to use the technology.

Moreover, the Rukhiran et al. (2023) study shows that the perceived usefulness of biometric systems positively influences students' adoption of such systems, leaving no doubt that in an academic setting, usefulness is still a major factor. Identical results to these were found by Wahid and Pratama (2022) It was shown that the more users thought that biometric authentication would help to protect their devices and provide an easier way to access them.

In summation of previous studies, usefulness perception is a significant key to determining intent to use biometric authentication. Once they think technology is easy to use and has enough usefulness for them.

2.2.2 Perceived Ease of Use (PEOU)

Perceived ease of use (PEOU) is defined as the perception that a particular system is simple and easy to use without requiring much learning (Davis, 1989). Within technology adoption studies, PEOU has been shown to have a direct relationship to consumers' behavioral intentions (BI). This means that users are more likely to adopt a system when they find it simple and easy to use.

As Wang (2021) studied 264 international students with prior engagement using biometric technologies in FinTech applications, the results show that PEOU is in decision adoption. This indicates that biometric technologies are working in technology, effortless systems, and authentication processes.

In the same way, the results from Zhang (2024) demonstrate that consumers who perceive ease of use associated with integrated facial recognition payments tend to retain stronger confidence in its usefulness and, as such, are more inclined to embrace its use. Such results suggest that the ease of use may not necessarily be a design or technical attribute, but rather a design or technical and psychological element that contributes to its acceptance.

Moreover, Faqih and Jaradat (2015) suggest that older users of integrated mobile healthcare services encounter pronounced cognitive challenges and,

consequently, heightened security and privacy concerns. According to Liu et al. (2025) demonstrated that older adults show less interest in Facial recognition systems for payment due to privacy issues. Privacy, trust and security issues are creating barriers to adoption due to perceptions regarding the ease of use (PEOU). In summary, existing literature provides strong evidence that PEOU is a key variable influencing consumers' intention to adopt biometric authentication. Nevertheless, variations across age groups and contexts suggest that the role of PEOU may not be uniform.

In summary, existing literature provides strong evidence that PEOU is a key variable influencing consumers' intention to adopt biometric authentication. Nevertheless, variations across age groups and contexts suggest that the role of PEOU may not be uniform.

2.2.3 Security and Privacy Risks (SPR)

Security and Privacy Risks (SPR) refer to consumers' concerns about potential data misuse, identity theft, and privacy violations when using biometric systems. According to research from Dhagarra et al. (2020), Wang (2021) and Stylios et al. (2022), biometric authentication and digital financial services carry a plethora of risks which negatively impact the likelihood of individuals adopting these technologies. Based on previous studies that examined how perceived ease of use (PEOU) and perceived usefulness (PU) relate to consumers decision-making models, it has been demonstrated that the higher the perceived security and privacy risk is to an individual, then the lower the chance of adoption. Therefore, researchers suggest that in order to have a complete Technology Acceptance Model (TAM), it should include a Security Privacy Risk (SPR) component, especially in cases where both the user trust as well as their data protection issues are at the forefront of consideration.

In a recent study by Wirawan and Utomo (2024) regarding Indonesian's acceptance of biometric systems used in an academic environment, it was shown

that perceived security was a positive influence on users' behavioural intentions, while privacy concerns were not found to have a significant influence. This indicates that if the environment is perceived as being a relatively controlled or low-risk environment, individuals will place greater importance on the assurance of security over their concern for privacy. However, with Chinese consumers, as presented in a study by Nan et al. (2022), it was demonstrated that perceptions of risk reduce significantly the likelihood of adopting facial recognition payment systems as a result of uncertainty regarding data protection, which represents a significant barrier to adoption.This shows that privacy and security are not just technical issues, but also psychological barriers that users are concerned about.

Additionally, awareness of security and privacy risks increased the perceived usefulness because users think biometric systems effectively protect their valuable assets and personal information (Stylios et al., 2022). Overall, while security and privacy risks are approaching an increasing importance, they do not have the same impact on all situations, as users will have a greater willingness to adopt biometric systems when they feel secure than to when they have security and/or privacy issues associated with adopting biometric technologies.

2.2.4 Behavioural intention to adopt biometric authentication (BI)

Behavioral intention (BI) refers to how motivated or willing a person is to use a technology. It is often shown to be the strongest factor influencing whether people will use it (Rukhiran et al., 2021; Noori & Jailani, 2022). In the case of biometric authentication, the link between intention and actual usage is even more important, since the decision to use the technology often depends on whether people trust the system and feel that it fits into their daily lives. For example, in a study of 161 first-year students in Thailand, behavioral intention was showing a very strong positive effect on actual system apply of biometric attendance technology (β = 0.938, P-value less than 0.001). This suggests that when students have stronger intentions, they are more likely to translate them into actual use (Rukhiran et al., 2023).

In addition, a study in the Netherlands examined a CBT-I mobile app in the healthcare field and found that the participants whose intention was positive used the app significantly more than the other participants (Fitrianie et al., 2021). The study found that BI was an integral component that connected app enjoyment to actual usage. Also, BI was the strongest predictor of AU of biometric authentication systems (beta = 0.459, P < 0.001), explaining 57.7% of the variability in usage behavior (Wirawan & Utomo,2024).

These results confirm that, while BI predicts actual adoption in all cases, the strength of this relationship is context-dependent, which suggests that a lack of environmental readiness, security perceptions, and culture surrounding the context could explain the relative absence of actual usage. The way BA influences the actual usage of the app shows the same trends in educational and healthcare studies. In these studies, BI consistently shows a positive impact on actual usage, although the strength of this relationship varies across educational and healthcare settings.

2.2.5 Actual Usage Behavioural to adopt biometric authentication (AU)

Actual usage behavior refers to the level to which users engage with biometric authentication in their daily lives. For example, it includes whether individuals use biometric systems such as fingerprints, facial recognition, or other biometric systems for secure access. Prior research showed that several factors such as PU, PEOU, SPR, and behavioral intention (BI) will influence actual usage.

PU and PEOU generally promote adoption. When biometric systems are seen as efficient and convenient. to operate, users are more likely to adopt them in practice. According to Fitrianie et al. (2021) conducted a study in the Netherlands with 89 participants to examine adoption of a mobile CBT-I app. The results showed that ease of use significantly influenced behavioral intention (β = 0.45, P-value less than 0.05), while behavioral intention in turn significantly predicted actual use (β = 0.41, P-value less than 0.05). These studies indicate when consumers believe a

system is simple to use, they are more likely to adopt it, and this intention directly translates into real adoption.

Similarly, Rukhiran et al. (2023) investigated the adoption of a facial recognition attendance system among 161 first-year university students in Thailand. They found that there was a statistically significant relationship between an individual's perceived utility from using the biometric system and his or her intent to be a user (beta = 0.169; p=0.036) while users' intent to use the biometric system also had an extremely positive effect on the actual usage of biometric systems (beta = 0.938; $p < 0.001$). This indicates that when users perceive the benefits of the biometric systems they are using, their intent to adopt the systems will be highly converted into actual usage.

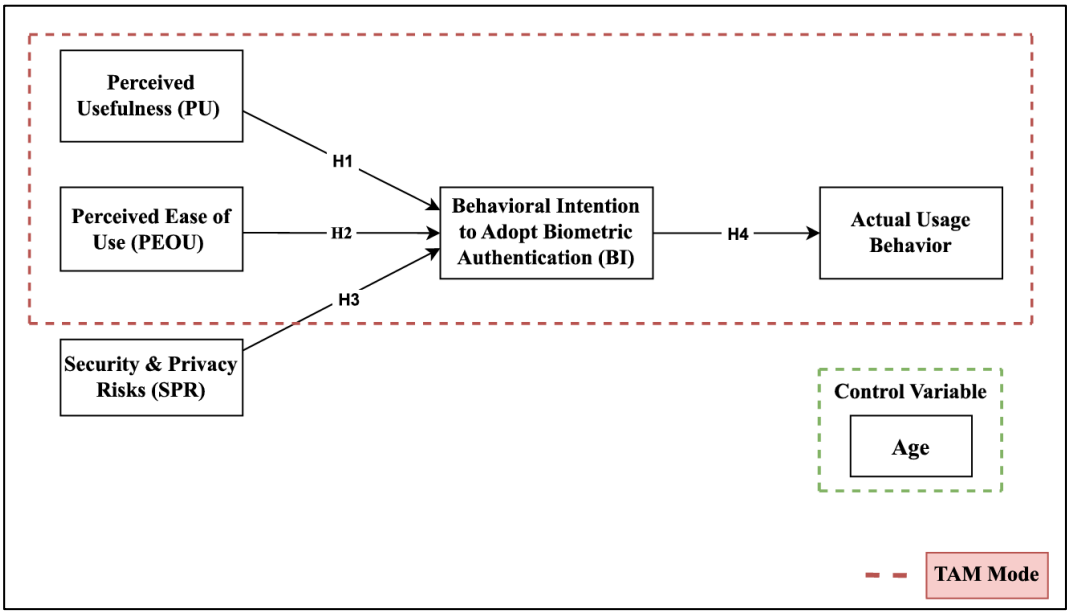
According to Rukhiran et al. (2023), in addition to evaluating the effect of using biometric authentication as a means of establishing identity, they also studied how trustworthy users perceive biometric systems and showed that trust is positively related to user intention. The relationship between perception of trust in a biometric system and intention to use a biometric system is significant (beta = 0.115, p = 0.194) The researchers did find that when the individual develops behavioral intention (the commitment to engage), it is a strong predictor of actual usage (beta=0.938, $p<0.001$). This indicates that while there may be instances when security and privacy factors don't impact how someone intentions to use something, the development of behavioural intention is still a strong This indicates that while there may be instances when security and privacy factors don't impact someone's intentions to use something, the development of behavioural intention is still a strong predictor of actual adoption.

These findings support the notion that both perceived usefulness and perceived ease of use are driving factors behind using biometric authentication, while the security and privacy factors related to using biometric authentication may affect adoption efforts but are not consistently statistically significant across different user contexts. In addition, a person's behavioural intention is the strongest predictor of actual biometric authentication usage, although that prediction may vary based on context. Adoption rates in educational institutions tend to be higher

than adoption rates in the healthcare and low-trust contexts, which speaks directly to the importance of context as it relates to security and privacy.

2.3 Conceptual Framework

Figure 2.2:



[H1] Perceived Usefulness (PU) has a significant influence effect on consumers' behavioral intention to adopt biometric authentication.

[H2] Perceived Ease of Use (PEOU) has a significant influence effect on consumers' behavioral intention to adopt biometric authentication.

[H3] Security and Privacy Risks (SPR) have a significant influence effect on consumers' behavioral intention to adopt biometric authentication.

[H4] Behavioral intention to adopt biometric authentication has a significant influence effect on actual usage behavior.

2.4 Hypotheses Development

2.4.1 Perceived Usefulness (PU)

Several prior studies consistently demonstrate that PU acts an important role in affecting users' willingness to adopt biometric authentication. According to Stylios et al. (2022), discovered that PU has a significant positive effect on behavioural intention (β = 0.181, p < 0.05). Similarly, Rukhiran et al. (2023), reported a significant positive relationship between PU and behavioural intention (β = 0.169, p = 0.036). Consistent evidence was also provided by Similarly, Sultana and Akter (2025) concluded that perceived value has a strong favorable effect on behavioral intention toward adopting IoT-based biometric technology (β = 0.431, p < 0.05). Overall, these studies consistently show that perceived usefulness strongly drives consumers' intention to adopt biometric authentication. Therefore, the hypothesis was made:

[H1] Perceived usefulness (PU) positively influences consumers' behavioural intention to adopt biometric authentication.

2.4.2 Perceived Ease of Use (PEOU)

Perceived ease of use be an essential component in affecting users' behavioural intention to adopt biometric technologies. When biometric systems are design to be simple, intuitive, and effortless, users tend to develop stronger intentions to adopt them. According to Zhang (2024), reported that PEOU had considerable beneficial impact on behavioural intention toward facial recognition payment ($\beta = 0.317$, $p < 0.05$). Furthermore, Liu et al. (2025) concluded that the perceived ease of using biometric systems has a positive effect on users' attitudes towards the application of biometric systems (Beta = 0.21, p<.001). This indicates that the perceived ease of using these systems increases the likelihood that users will use these systems, due to the reduced cognitive effort associated with using the systems. Similarly, Sultana and Akter (2025) confirmed that perceived ease of use has a significant and beneficial effect on behavioural intention to adopt Internet of Things (IoT) based biometric devices (beta = 0.404, $p < 0.001$). Therefore, the hypothesis was made:

[H2] Perceived Ease of Use (PEOU) has a significant influence on consumers' behavioral intention to adopt biometric authentication.

2.4.3 Security and Privacy Risks (SPR)

Several empirical studies indicate that SPR is an important variable in shaping consumers' behavioral intention to utilize biometric authentication technologies. According to Wirawan and Utomo (2024), security perception has a positive impact on behavioral intentions, with a beta of 0.368 and a p-value less than .001; that indicates that if it is perceived as being more secure, then the greater the intention to adopt the technology. In contrast, Nan and colleagues (2022) concluded that an increase in user perceived risk would lower the ambition to implement biometric payment systems by displaying a beta value of -0.157, with a statistical significance of $p < 0.001$ in relation to this relationship. Therefore, when customers perceive greater levels of insecure and private transactions, this ultimately leads to a decrease in their intention to utilize such technologies.

On the other hand, Stylios et al. (2022) provided evidence that perceived risk had a positive, although statistically insignificant, effect on the adoption

intention (beta = 0.11, p-value = 0.281), which could mean that the influence of security and privacy risks will differ in different contexts. Therefore, the conclusion of the study indicates that perceived security may lead to enhanced behavioral intention, but that security and privacy risks typically function as barriers to adoption. Thus, the following hypothesis was developed:

[H3] Security and Privacy Risks (SPR) have a significant influence effect on consumers' behavioral intention to adopt biometric authentication.

2.4.4 Behavioural intention to adopt biometric authentication (BI)

Behavioral intention is one of the strongest predictors of actual system usage across biometric and digital technology contexts. According to Rukhiran et al. (2023) reported a very strong positive effect of behavioral intention on actual usage (β = 0.938, $p < 0.001$).Similarly, Fitrianie et al. (2021) found that behavioral intention significantly predicted actual usage ($\beta = 0.41$, $p < 0.05$), while Wirawan and Utomo (2024) confirmed that behavioral intention strongly influenced actual usage behavior ($\beta = 0.459$, $p < 0.001$).Overall, these findings indicate that strong behavioral intention reliably leads to higher levels of actual biometric system usage. Therefore, the hypothesis was made:

[H4] Behavioral intention to adopt biometric authentication has a significant influence effect on actual usage behavior.

2.4.5 Control Variable

Age acts as a control variable because users from different generations naturally differ in digital literacy and familiarity with biometric technologies.

Table 2.0 Type of generation

Type of generation	**Year of Birth**	**Current Age**
Silent Generation	1925-1945	80-100
Baby Boomers	1946-1964	61-79
Generation X	1965-1980	45-60
Millennials	1981-1996	29-44
Generation Z	1997-2012	13-28
Generation Alpha	2013-2028	12 maxes

Younger users are more comfortable engaging with systems like fingerprint and facial recognition. Conversely, older users show more wariness and find these systems harder to engage with. Prior studies support these trends. Hung and Jen (2012) found younger users were more likely to adopt new technologies, and Natarajan et al. (2018) found that younger users had easier experiences than older users when using a particular technology. According to Gao et al. (2025), older users were more sensitive to risk when using a technology such as facial recognition for payments and were therefore less willing to use such technologies. Even though these differences do not change the theory, they may still affect behavior. Therefore, control for age to minimize demographic bias and to produce more accurate data on actual user behavior.

2.5 Research Gap

Although previous studies have widely applied TAM to explain technology adoption, several gaps remain in the context of biometric authentication. First, the many studies done on biometric authentication in Malaysia are still very few. An example of this is Ali et al. (2021), who sampled the objectives of Malaysian clientele who are attempting to use cardless banking technology, while Ruhani et al. (2024) developed a framework to address security concerns and user behavior related to e-wallet adoption. These studies show that prior technology adoption research in Malaysia has mainly focused on general mobile applications or e-wallet

services, with very few examining biometric authentication specifically. This gap suggests that our understanding of biometric technology uptake in Malaysia is still limited, which warrants dedicated investigation.

Moreover, prior research mainly focuses on PU and PEOU, but the role of security and privacy risks (SPR) has received less attention, even though it is an important concern for users. Many biometric technology adoption research studies have utilized student sample populations, which are often not representative of the general population. For example, Faqih and Jaradat (2015) reported that more than half (60%) of their sample was between the ages of 20 and 29, while fewer than 10% of the participants were 40 years of age or older. This means that a significant amount of biometric technology adoption research has focused on younger individuals, making it difficult to extrapolate the findings to other age groups. As well, many research appendices do not provide detail on how age is related to biometric technology adoption patterns, creating uncertainty regarding the influence of age on biometrics and technology adoption.

Furthermore, the practicality of utilizing biometric authentication systems has not often been explored. An example of this would be an individual who has worn down their fingers to such an extent that fingerprinting is impossible. Therefore, this individual cannot use their fingerprint for biometric authentication. Additionally, the use of face recognition systems may be affected by environmental variables such as poor lighting. Thus, users may need to attempt several times before completing the transaction as well as having trouble navigating through the system efficiently. Prior studies have suggested that there are barriers to adopting biometric authentication systems. For example, several groups of individuals may have difficulty obtaining fingerprints, and environmental variables impact the accuracy of face recognition. Both factors will lead to poor experience for potential biometric users (Lien & Vhaduri, 2023). These limitations highlight that the application of biometric technology depends not only on cognition but also on its actual usability.

Therefore, this study aims to explore the adoption of biometric authentication in Malaysia by integrating PU, PEOU, and SPR into a single framework and incorporating age as a control variable to address these shortcomings. In doing so, this study can provide a more comprehensive and practical insight into consumers' willingness to adopt biometric authentication.

2.6 Conclusion

This chapter studies the dependent variable, actual usage of biometric authentication, and the independent variables, perceived usefulness (PU), perceived ease of use (PEOU), security and privacy risks (SPR), and behavioural intention (BI). The Technology Acceptance Model (TAM) is adopted as the theoretical foundation to explain the relationships among these variables. The conceptual framework illustrates how these factors influence the actual usage of biometric authentication in the Malaysian context. Based on the reviewed literature, a set of hypotheses was developed to guide the empirical analysis.

CHAPTER 3: METHODOLOGY

3.0 Introduction

In this part of methodology covers research design, sampling strategy, data collection methods, and proposed data analysis tools. As the research is based on primary data gathered through a structured questionnaire, it particularly focuses on explaining the process of data collection and how the data was used to test the hypotheses established earlier.

3.1 Research Design

This study uses a quantitative, cross-sectional design to explore what affects consumers' intention to adopt biometric authentication in Malaysia.A quantitative method is suitable for this study because it enables the measurement of relationships among variables using numerical data and allows the proposed hypotheses to be tested statistically. According to Saunders et al. (2016), research surveys can collect detailed quantitative (numerical) data from large groups of respondents, which can help the study in thoroughly testing all hypotheses.

Respondents evaluated their perceptions of PU, PEOU, SPR, behavioral intention, and actual usage of biometric authentication. The study includes both descriptive and causal analyses. Descriptive analysis outlines the basic demographic characteristics of respondents, particularly age, and their attitudes toward biometric authentication. Causal analysis examines the relationships between the independent variables (perceived usefulness, perceived ease of use, and security and privacy risks) and the dependent variables (behavioural intention and actual usage behaviour). Age is incorporated as a control variable to ensure that demographic differences do not bias the relationships among the constructs. Additionally, age groups were created to allow group-based comparisons in the structural model such as young, middle-aged, and older adults. The specific age

ranges for each group are defined and justified in Chapter 4 during the data analysis process.

This research design aligns with previous studies that utilize the Technology Acceptance Model (TAM) which commonly employ quantitative, survey-based, and causal approaches to investigate user acceptance of new technologies. Therefore, the selected research design enhances the reliability, validity, and generalizability of the findings to a broader population of Malaysian users.

3.2 Data Collection Methods

3.2.1 Primary Data

Primary data refers to first-hand information collected directly by the researcher that has not been previously published or influenced by external sources. Due to its originality, primary data is regarded as more accurate, reliable, objective, and credible than secondary data (Taherdoost, 2021). In this study, primary data was collected using Google Forms, a widely used and effective platform for designing online questionnaires and collecting responses conveniently and efficiently.

The platform is user-friendly for researchers and respondents. It automatically records all submissions into an integrated spreadsheet. This feature allows researchers to review data immediately without manual entry. The platform also provides basic summary charts for quick preliminary analysis. For respondents, it is simple, intuitive, and easy to use. This encourages higher participation and supports efficient data collection.

This method of primary data was selected because it is widely recognized as effective for behavioral studies, as it allows researchers to collect structured data directly from sources such as surveys, observations, case studies, and interviews, thereby aligning with the study's research objectives (Ajayi, 2023). Furthermore, most previous studies have also relied on survey questionnaires to measure

consumers' intention to adopt biometric authentication (Suh & Han, 2002; Faqih, 2021; Stylios et al., 2022). In this study, all participants understood the purpose of the research and participated voluntarily. The study also emphasized the protection of privacy and confidentiality in accordance with the Personal Data Protection Act 2010 (PDPA), ensuring that no personally identifiable data were misused and that all information was used strictly for research purposes.

3.3 Sampling Design

3.3.1 Target Population

The target population of this study consists of Malaysian residents aged below 28 to above 80 who have experience using biometric authentication in their daily lives, particularly through applications such as mobile banking, e-wallets, and other digital payment services. The questionnaire was designed so that only respondents who indicated prior use of biometric authentication were allowed to continue completing the survey. According to Miskan et al. (2021) highlighted that demographic factors, particularly age, significantly influence perceptions and acceptance of biometric security. Therefore, including respondents across a wide age range enables the study to capture demographic differences that may affect individuals' perceptions and behavioural intentions toward biometric authentication.

The age categories were designed based on generational classification to capture differences in biometric authentication adoption. Respondents aged 28 and below represent Generation Z, who are widely recognized as digital natives with high exposure to smartphones, mobile banking, and biometric-enabled technologies (Safuri et al., 2024).In contrast, older age groups represent earlier generations who differ in digital literacy, familiarity with financial technologies, and sensitivity to security and privacy risks, which may influence their adoption behavior. An open-ended upper age category (above 80) was adopted to avoid imposing an arbitrary age ceiling and to ensure the inclusion of older users, as prior fintech studies

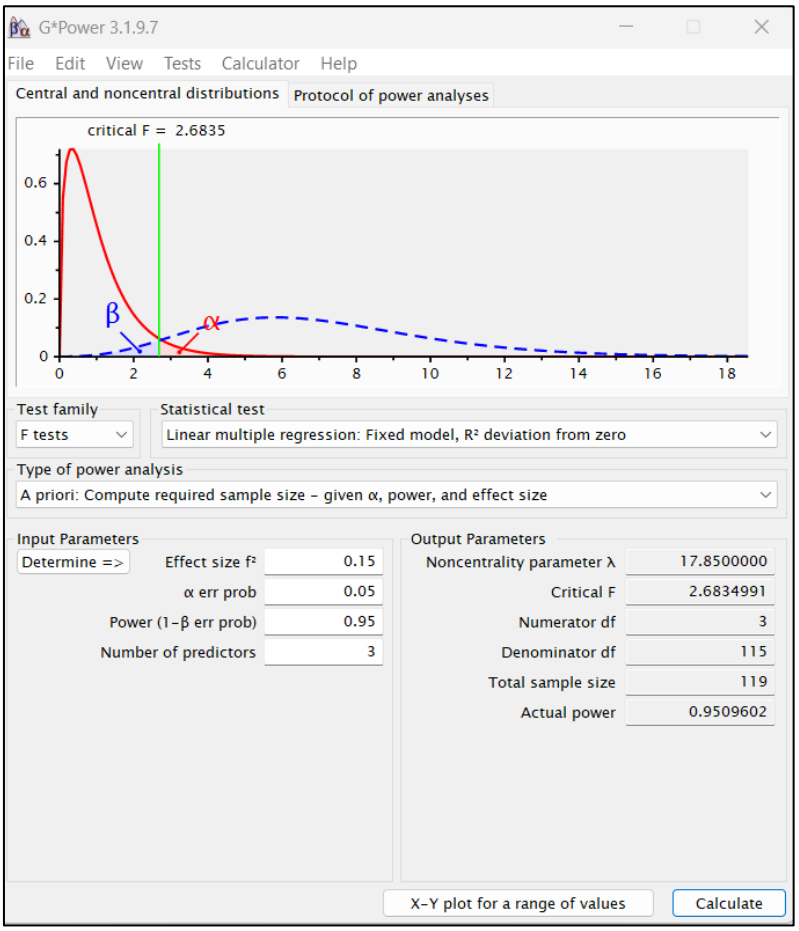
highlight that elderly consumers exhibit distinct technology anxiety and adoption patterns that should not be excluded from analysis (Han & Ko, 2025).

3.3.2 Sample size

Sample size refers to the subset of a population selected to ensure that sufficient information is collected to draw reliable conclusions (Sekaran & Bougie, 2010; (Memon et al., 2020). Choosing an appropriate sample size is important, because a small sample may reduce the accuracy and trustworthiness of the results, while a large sample may lead to unnecessary use of time and resources (Hamad & Ahmed, 2025).According to Fadiya (2018),researchers recommendations suggest having at least 150 cases or around 5 to 10 cases for each variable in the analysis to produce stable multivariate results.

Based on these guidelines, this study also conducted a G*Power analysis using three number of predictors, an effect size of 0.15, a significance level of 0.05 and a power level of 0.95. The analysis showed that a minimum of 119 respondents was needed to achieve adequate statistical power. The G*Power output is presented in Figure 3.0.

Figure 3.1: Result of G*Power



Source: Author's own data analysis from G*Power

Based on both the literature guidelines and the G*Power result, the study targeted 300 to 400 respondents to ensure strong and reliable findings. In total, 324 valid responses were collected, which is higher than the minimum requirement and suitable for behavioural studies and PLS-SEM analysis. The data were first analysed using SPSS for measurement assessment and later processed in SmartPLS to test the structural model, following approaches used in previous studies (Khayer, 2024; Md Kassim, 2024).

3.3.3 Sampling Frame and Location

The sampling frame of this study consists of Malaysian residents who have experience using biometric authentication. Data was collected using a hybrid approach that involved both online and physical distribution of the questionnaire.

For physical data collection involved distributing printed QR code cards linked to the survey to invite participants directly. At Universiti Tunku Abdul Rahman (UTAR), particularly around the KA and KB Blocks, individuals were approached and requested to scan the QR code to complete the questionnaire. This method was also implemented in other public settings, such as food courts and cafés near the university, as well as in Tangkak, Muar, and Penang, where individuals were similarly invited to participate by scanning a QR code.

In addition, the online sampling frame was created through the distribution of the questionnaire link across various social media platforms, including Facebook, WhatsApp, Instagram Stories, WeChat and Microsoft Teams. The survey was also shared with students, lecturers, working adults and older individuals, allowing it to reach a wider range of respondents across Malaysia.

This combined online and physical sampling approach enabled access to a diverse group of participants across different demographic backgrounds. Similar methods have been adopted in previous Malaysian studies on digital payment and facial-recognition payment adoption (Wan Nawang & Syabil Nazhan Ahd. Moess, 2023; Mohd et al., 2025). Although non-probability sampling may limit generalizability, it remains suitable for exploration technology adoption research.

3.3.4 Sampling Technique

This study used non-probability sampling, mainly convenience sampling and snowball sampling. Convenience sampling was chosen because it allowed participants to be selected based on who was available and willing to take part, which was practical due to time and resource limitations (Etikan, 2016). This method was used when inviting individuals at UTAR (KA and KB Blocks), and at food courts and cafés in Tangkak, Muar, and Penang, to scan the QR code and complete the survey.

Snowball sampling was also applied, as the survey link was shared through social networks and academic channels. This helped the study reach more people, including students, lecturers, working adults and older individuals from different states in Malaysia. Although non-probability sampling may limit how well the results can be generalized, it is still suitable for exploration studies on technology adoption (Showkat & Parveen, 2017).

3.4 Research Instruments

3.4.1 Questionnaire Design

The research instrument used in this study was a self-administered questionnaire which was designed to collect primary data and information from the respondents. The questionnaire consisted of two sections, which are A and B. Section A gathered demographic information such as gender, age, and education level, which provided background characteristics and allowed examination of possible demographic influences on biometric authentication adoption.

Section B measured the constructions in the proposed research framework. The independent variables (IVs) in this study were Perceived Usefulness (PU), Perceived Ease of Use (PEOU), Security and Privacy Risks (SPR), and Behavioural Intention (BI) when predicting Actual Usage Behaviour (AU). Behavioural Intention (BI) also functioned as an endogenous variable, acting as the dependent

variable for the relationships involving PU, PEOU, and SPR. The dependent variable (DV) of the study was Actual Usage Behaviour (AU). Age was included as a control variable to examine whether demographic differences influence the strength of the relationships among the constructions. All measurement items were adapted from established scales used in prior technology adoption studies to ensure validity and relevance to biometric authentication.

All items in Section B were measured using a five-point Likert scale ranging from 1 = Strongly Disagree to 5 = Strongly Agree, a format widely used for capturing respondents' level of agreement in behavioral research (Sharma, 2016). This scaling method was chosen because it is simple, reliable, and effective for quantifying perceptions and attitudes.

The questionnaire was reviewed and refined under the supervision of the project supervisor before being distributed online via Google Forms. A summary of the measurement items and their original sources is presented in Table 3.1 and 3.2.

Table 3.1: 5-point Likert scale

5-point Likert scale				
1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Source: (Sharma, 2016)

Table 3.2: Questionnaire Section B

Constructs	Original	Modified	Source
Perceived Usefulness (PU)	1) Using this Internet banking site enhances the productivity of my banking activities." (Suh & Han, 2002) 2) Using this Internet banking site enables me to accomplish banking activities more quickly." (Suh & Han, 2002) 3) Using mobile phone would improve my performance in conducting m-healthcare behaviours (Faqih,2021) 4) Using mobile phone would make it easier for me to perform m-healthcare behaviours. (Faqih,2021) 5) I would find the mobile phone useful in performing m-healthcare behaviours. (Faqih,2021)	1) Using biometric authentication enhances the productivity of my digital financial activities. 2) Using biometric authentication enables me to accomplish tasks more quickly. 3) Using biometric authentication provides valuable benefits for me 4) Using biometric authentication makes it easier for me to carry out activities. 5) I find biometric authentication useful in performing my activities such as secure financial and digital activities.	1) (Suh & Han, 2002) 2) (Faqih,2021)

Perceived Ease of Use (PEOU)	1) BBCA technology will require little effort. (Davis, 1989) 2) Learning to use BBCA technology would be easy for me. (Davis, 1989) 3) I find it easy to get this Internet banking site to do what I want it to do. (Suh & Han, 2002) 4) My interaction with this Internet banking site is clear and understandable. " (Suh & Han, 2002) 5) It would be easy for me to obtain what I need by using mobile phone to perform m-healthcare behaviours. (Faqih,2021)	1) It is easy for me to use biometric authentication. 2) Learning to use biometric authentication would be easy for me. 3) I find it easy to get biometric authentication to do what I want it to do. 4) It is clear and easy for me to understand how to use biometric authentication. 5) It is easy for me to accomplish what I need by using biometric authentication.	1) (Davis,1989) 2) (Suh & Han, 2002)

Security and Privacy Risks (SPR)	1) It is likely that someone may get access to my bank account by stealing my phone and/or violating its access control mechanism. (Stylios et al., 2022) 2) It is likely that someone may break into my social media and e-mail accounts. (Stylios et al., 2022) 3) It is likely that someone may use my mobile for e-payments. (Stylios et al., 2022) 4) I may get unauthorized charges on my bank account. (Belanger and Carter, 2008) 5) It is likely that someone may steal my device and gain access to my personal data, photos and videos stored in it. (Stylios et al., 2022)	1) It is likely that someone may get access to my accounts by bypassing biometric authentication. 2) It is likely that someone may break into my online accounts by bypassing biometric authentication. 3) It is likely that someone may use biometric authentication on my device for unauthorized payments. 4) I may get unauthorized charges on my accounts even when using biometric authentication. 5) It is likely that someone may steal my device and gain access to my personal data even with biometric authentication.	1) (Stylios et al., 2022) 2) (Bélangeran d Carter, 2008)
Behavioural intention to adopt Biometric	1) I should apply this BBCA technology as Soon as	1) I intend to adopt Biometric Authentication	1) (Davis,1989) 2) (Rukhiran et al., 2023)

Authentication (BI)	possible Davis (1989) 2) I prefer biometric recognition for examination attendance than the traditional method. (Rukhiran et al., 2023) 3) I will use facial biometric recognition when I have an examination attendance (Rukhiran et al., 2023) 4) I intend to use the mobile phone to perform m-healthcare behaviours frequently. (Faqih,2021) 5) It is likely that I will use the mobile phone to perform m-healthcare behaviours in the future. (Faqih,2021)	technology as soon as possible. 2) I prefer biometric authentication over traditional methods (e.g. Passwords/PINs). 3) I will use biometric authentication whenever it is available (e.g., when I need to verify my identity). 4) I intend to use the mobile phone to perform Biometric Authentication behaviours frequently. 5) It is likely that I will use my mobile phone to perform biometric authentication in the future.	3) (Faqih,2021)
Actual use behaviour to adopt biometric authentication	1) I would use a face recognition system for examination attendance.	1) I have used biometric authentication when it is available.	1) (Ganguly & Ghosh, 2025) 2) (Rukhiran et al., 2023)

	(Rukhiran et al., 2023) 2) I use m-banking frequently. (Ganguly & Ghosh, 2025) 3) I am very likely to use the Mobile Banking App in the future. (Khan, Rana, & Hosen, 2021) 4) I believe it is worthwhile for me to use the Mobile Banking App. (Khan, Rana, & Hosen, 2021) 5) I would recommend my university use a face recognition system for student identification in all authentication areas. (Rukhiran et al., 2023)	2) I have used biometric authentication many times during a typical week. 3) I am very likely to continue using biometric authentication in the future. 4) I think using biometric authentication is worth it. 5) I would recommend using biometric authentication to others.	3) (Khan, Rana, & Hosen, 2021)

3.4.2 Pilot Test

A pilot test aims to evaluate the feasibility of a method intended for use in a larger-scale study. Furthermore, it serves as an important step in determining whether a chosen method is suitable for larger-scale research. Research studies of every type

are encouraged to include a pilot stage to ensure that instruments are effective before the main data collection (Leon et al., 2011).

In this study, a pilot test has been applied to evaluate the clarity, validity, and reliability of the questionnaire. The test aims to assess whether the questions were easy to understand, ensure respondents captured the needed information and prevent missing nothing important. After can based on the on the feedback, Afterwards, the questionnaire was improved, revised, and perfected based on the feedback. The Cronbach's Alpha was applied to determine the instrument's reliability in this study. According to table 3.1, it shows level acceptance of the Cronbach Alpha coefficient.

.

Table 3.3: Rules of Thumb about Cronbach Alpha Coefficient

Cronbach's alpha	**Internal consistency**
$\alpha \geq 0.9$	Excellent
$0.9 > \alpha \geq 0.8$	Good
$0.8 > \alpha \geq 0.7$	Acceptable
$0.7 > \alpha \geq 0.6$	Questionable
$0.6 > \alpha \geq 0.5$	Poor
$0.5 > \alpha$	Unacceptable

Source: (Sharma, 2016)

For this study, 30 questionnaires were distributed. Responses were analyzed using IBM SPSS to measure construct consistency, and Cronbach's Alpha was calculated. According to Sharma (2016), Cronbach's Alpha values greater than 0.7 are generally considered acceptable for reliability, with values above 0.8 being good and above 0.9 being excellent (Table 3.2).

Table 3.4: Results of the Pilot Test

Variable	**Cronbach Alpha's**	**No. of Items**	**Strength of Association**
Perceived Usefulness (PU)	0.888	5	Good

Perceived Ease of Use (PEOU)	0.921	5	Excellent
Security and Privacy Risks (SPR)	0.924	5	Excellent
Behavioral Intention (BI)	0.891	5	Good
Actual Usage Behaviors (AU)	0.927	5	Excellent

Source: Developed of the research

Table 3.3 shows that all independent variables have strong positive relationships with the dependent variable. Based on the results shown above, the strongest associations are with PU (0.888), PEOU (0.921), SPR (0.924), BI (0.891), and AU (0.927). The Cronbach's Alpha for all variables is greater than 0.7, meaning that all variables are reliable for this study.

3.5 Constructs Measurement

3.5.1 Nominal Scale

Nominal scales are the simplest form of measurement and classify variables into categories based on shared qualitative attributes (Idika et al., 2023). In this study, nominal scales were used to measure several demographic variables, including gender, age and education level. Respondents selected the category that best described their characteristics.

By applying nominal scaling, researchers can generate data from different respondent groups for descriptive analysis and to analyze potential differences between categories. These demographic variables are crucial for understanding sample characteristics and determining whether specific characteristics, especially age, influence the adoption of biometric authentication.

3.5.2 Interval Scale

An interval scale is a type of measurement where the gaps between numbers are equal, but zero does not mean "nothing." This allows differences between responses to be compared in a meaningful way (Stevens, 1946). An interval scale was used in this study to measure both the dependent and independent variables. Each question was rated on a Likert scale ranging from 1 = Strongly Disagree to 5 = Strongly Agree, which is one of the most common formats used in surveys and questionnaires (Church & Waclawski, 1998; Fink, 1995). This method offers quantitative data appropriate for statistical analysis, including regression analysis, correlation, and descriptive statistics, and enable respondents to express their degree of agreement with each conclusion.

3.6 Data Processing

This section explains the steps taken to prepare the collected data before conducting statistical analysis. Data processing ensures that the dataset is accurate, complete, and ready to be analyzed using SmartPLS.

3.6.1 Data Checking

Before distributing a survey questionnaire to participants, the researcher should first review it thoroughly. This will allow the researcher to find any errors or problems in the questionnaire. By correcting these errors or problems, the researcher will be able to produce the most accurate information possible when conducting their research.

3.6.2 Data Editing

Data editing involves reviewing collected data for consistency, identifying errors and outliers, and making corrections to improve its value for research (Naeem, 2019). After data collection, responses were examined to identify issues such as missing information, duplicate entries, or inconsistent answers. Any irregularities were carefully evaluated to maintain data accuracy and reduce potential bias. This process ensured that the dataset was clean, reliable, and ready for subsequent statistical analysis.

3.6.3 Data Coding

Data coding is an essential step in quantitative data preparation. It involves assigning numerical values to participants' responses in order to systematically record, organize, and analyze the information. According to Sekaran and Bougie (2016), identified coding as a process that converts unstructured data into a structured format for use with statistical analyses or software programs. Similarly, through the use of coding, data collected through electronic surveys can be categorized into one set of standardized numerical values, which help clarify confusion when working with high numbers of questions on an instrument.

The data that was exported from Google Forms as a spreadsheet was organized within Microsoft Excel for easy tracking of where each response corresponds to each question. Demographic data in first section A was assigned a numerical value representing variables such as "gender," "age group," and "level of education". In the second section B, the ratings on the Likert scale (1=strongly disagree to 5=strongly agree) were assigned numerical codes that could later be processed consistently in SmartPLS for both measurement model and structural model analysis.

3.7 Data Analysis

Data analysis is the systematic process of cleaning, transforming, and structuring data to draw clear and accurate conclusions. The objective is to present information in a clear, conclusive, and accessible format to minimize the risk of misunderstanding. (Islam, 2020). Partial Least Squares Structural Equation Modeling (PLS-SEM) in SmartPLS 4 was used in this study.It can handle complex models with multiple indicators and nonnormal data distributions, it is well-suited for behavioral research (Sultana & Akter, 2025). This section covers both descriptive and inferential analyses, where the measurement model and structural model were assessed using PLS-SEM to test the proposed hypotheses. Additionally, Age was also examined in greater detail during the structural analysis to explore whether the results differed across age segments.

3.7.1 Descriptive Analysis

Descriptive analysis involves cleaning, transforming, and structuring data to provide clear and understandable insights about a dataset (Rawat, 2021). It allows researchers to identify overall patterns, compare variables, and detect outliers in the data. Moreover, descriptive analysis helps address basic research questions related to “who,” “what,” “when,” and “to what extent” by offering a clear overview of the collected information (Loeb et al., 2017). The data from section A of the questionnaire will be presented in this study through tables and pie charts to provide an overview of the respondents' general characteristics and basic demographics.

3.7.1 Inferential Analysis

Inferential analysis is an approach of drawing conclusions about the target group as an entire through estimating and forecasting the sample data (Allanson & Notar, 2020). PLS-SEM was used for the actual hypothesis testing in this research, although multiple linear regression equations were used. The two main parts of the

analysis were the structural model assessment and the measurement model assessment.

3.7.1.1 Multiple Linear Regression

A statistical method called multiple linear regression (MLR) is used to search at the relationship between a particular dependent variable and multiple independent variables together. (Peter et al., 2019). This method allows researchers to assess how changes in several predictors collectively influence an outcome variable. According to Petchko (2018) further explained that multiple linear regression extends simple correlation analysis by estimating linear relationships between variables is described by a linear equation. According to Dawson et al. (2021), the general form of a multiple linear regression equation can be expressed as follows:

Figure 3.2: Equation of Multiple Linear Regression

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \varepsilon$$

Source: Dawson et al. (2021)

Where, Y is dependent variable; X1 and X2 are independent variables $\beta 0$ is the y-intercept (constant variable); $\beta_1, \beta_2, \beta_3$ are the slope coefficient, $\in$ is the residuals (also known as error term).This regression equation is presented to illustrate the linear relationships among the study variables, while the actual estimation and hypothesis testing were conducted using PLS-SEM in SmartPLS.

3.7.2.2Measurement Model Assessment

The measurement model was assessed in SmartPLS to ensure that all constructs met the required reliability and validity standards before proceeding to structural analysis. Outer loadings served to evaluate indicator reliability, and items with

loadings greater than the specified threshold of 0.70 were retained (Xue et al., 2011). Internal consistency reliability was evaluated using Cronbach's Alpha and Composite Reliability (CR), where values exceeding 0.70 indicated acceptable reliability (Nawi et al., 2022). Furthermore, the Average Variance Extracted (AVE) was used to verify convergent validity. AVE values above 0.50 were reached by all constructs, indicating that each construct effectively explained the variance in its indicators. (Nawi et al., 2022). Additionally, the HTMT ratio was used to examine discriminant validity; all HTMT values fall below the conservative threshold of 0.85, showing that the constructs were computationally distinct (Sultana & Akter, 2025). Overall, the results confirmed that the measurement model satisfied the required reliability and validity criteria.

3.7.2.3 Structural Model Assessment

SmartPLS was used to analyze the structural model and test the constructs hypothesized relationships. Path coefficients evolved, and their significance was tested using a bootstrapping process with 5,000 samples. Multicollinearity was examined using the Variance Inflation Factor (VIF). According to Daoud (2017), a VIF value of 1 indicates no connection between variables. Values below 5 show moderate correlation and indicate that multicollinearity is not a problem. However, values above 5 suggest high collinearity, which can increase standard errors and affect the accuracy of the coefficient estimates. The coefficient of determination (R^2) was used to assess the model's explanatory power, while effect size (f^2) was utilized to determine the impact of each predictor on the endogenous variables. Predictive relevance (Q^2) was assessed using the blindfolding procedure, with Q^2 values greater than zero indicating acceptable predictive capability (Wong, 2013). The relationships among variables in this study were analysed using PLS-SEM in SmartPLS, which estimates multiple regression-based relationships simultaneously, consistent with the linear relationship assumptions underlying the proposed research model

3.8 Conclusion

This chapter describes the methodology used in this study, including research design, sampling strategy, data collection procedures, measurement instruments, and data processing steps. It also described the analytical approach adopted using PLS-SEM in SmartPLS, including both the measurement and structural model assessments. These methodological procedures provide a systematic basis for analyzing factors that influence biometric authentication adoption among Malaysian users. The results are presented in chapter four.

CHAPTER 4: DATA ANALYSIS

4.0 Introduction

This chapter presents the analysis of the 324 valid responses collected for the study. Descriptive analyses are first used to summarise the respondents' demographic profile in Section A. For Section B, the measurement model and structural model are assessed using Partial Least Squares Structural Equation Modelling (PLS-SEM) in SmartPLS 4. In addition, the bootstrapping is conducted age-based intergroup comparisons to examine whether there were differences in structural relationships among young, middle-aged, and older respondents. The results are presented using tables and figures for clarity and effective interpretation.

4.1 Descriptive Analysis

4.1.1 Usage of Biometric Authentication (Screening Question)

Figure 4.1: Screening Question: Prior Use of Biometric Authentication

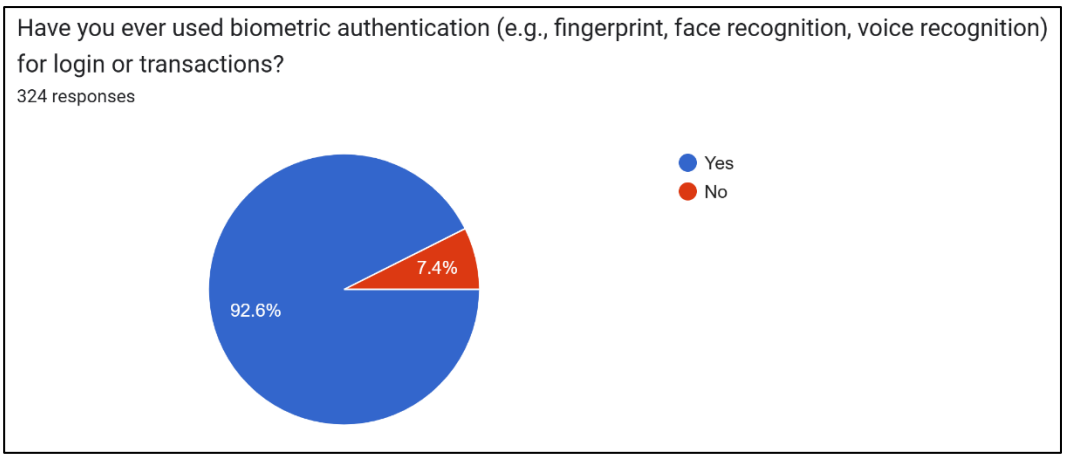


Figure 4.1 shows that out of 324 respondents, 92.6% (n = 300) reported having used biometric authentication, while 7.4% (n = 24) indicated that they had never used it.

As the study focuses on individuals with actual experience using biometric authentication, only those who selected "Yes" were allowed to continue with the full questionnaire. Therefore, all subsequent analyses including demographic statistics, the measurement model, and the structural model were conducted using the 300 valid responses.

4.1.2 Demographic Statistics

Table 4.1 Demographic profile of respondents

Demographic Data		**Frequency**	**Percentage (%)**
Gender	Male	137	45.7
	Female	163	54.3
Age	28 or less	106	35.3
	29 - 44	49	16.3
	45 - 60	52	17.3
	61 - 79	74	24.7
	80 and above	19	6.3
Education Level	Secondary / SPM / UEC	103	34.3
	Foundation	11	3.7
	Diploma	46	15.3
	Bachelor's Degree	127	42.3
	Master's Degree and above	13	4.3

Source: Author's own data analysis from Excel Sheets.

The demographic profile of the 300 valid respondents is presented in Table 4.1. The gender distribution consists of 45.7% (137 respondents) males and 54.3% (163 respondents) females. Age represents the most important demographic factor in this study, as it functions as the control variable. The largest age group consists of respondents aged 28 or less are 35.3% or 106 respondents, followed by those aged 61 - 79 (24.7% or 74 respondents), 45 - 60 (17.3% or 52 respondents), 29 - 44 (16.3% or 49 respondents), and 80 and above (6.3% or 19 respondents). In terms of

education level, 42.3% or 127 respondents their most respondents hold a bachelor's degree, followed by secondary-level qualifications such as SPM/UEC are 34.3% or 103 respondents, while another 46 respondents (15.3%) are Diploma level. On the other hand, master's degree and above are (4.3% or 13 respondents), and Foundation level are 11 respondents (3.7%). These demographic characteristics provide essential context for interpreting respondents' behavioural patterns toward biometric authentication.

4.2 Inferential analyses

4.2.1 Measurement Model Assessment

According to Chin's (1998) recommendations, item reliability is defined as individual item load Ings exceeding the 0.70 level. The research instrument successfully measured each construct separately in this investigation, since all 25 items attained outer loadings over this criterion (Table 4.2).

4.2.2 Item reliability

Following Chin (1998) guidelines, item reliability is determined by individual item load Ings exceeding the threshold of 0.70. In this study, all 25 items achieved outer loadings above this benchmark (Table 4.2), indicating that the research instrument effectively measured each construct independently. Consequently, all 25 items were retained for further analysis due to their statistical significance.

4.2.3 Internal consistency reliability

Table 4.2: Assessment of reliability and convergent validity

Constructs	**Items**	**Outer loadings**	**Cronbach's Alpha**	**Composite Reliability**	**Average Variance Extract-ed (AVE)**
Perceived Usefulness (PU)	PU1	0.926	0.957	0.967	0.852
	PU2	0.922			
	PU3	0.924			
	PU4	0.935			
	PU5	0.909			
Perceived Ease of Use (PEOU)	PEOU1	0.903	0.956	0.966	0.852
	PEOU2	0.937			
	PEOU3	0.924			
	PEOU4	0.923			
	PEOU5	0.927			
Security and Privacy Risks (SPR)	SPR1	0.9	0.959	0.968	0.859
	SPR2	0.934			
	SPR3	0.944			
	SPR4	0.921			
	SPR5	0.935			
Behavioural Intention to adopt biometric authentication (BI)	BI1	0.899	0.952	0.963	0.838
	BI2	0.906			
	BI3	0.917			
	BI4	0.921			
	BI5	0.934			
Actual usage behavior (AU)	AU1	0.913	0.956	0.966	0.852
	AU2	0.924			
	AU3	0.923			
	AU4	0.926			
	AU5	0.928			

Source: Author's own data analysis from SmartPLS.

Table 4.2 summarizes the estimated values for Cronbach's alpha and composite reliability as part of the internal consistency reliability evaluation. According to Sultana & Akter, (2025) indicate a minimum reliability requirement of 0.70. All of the constructions in this investigation achieved composite reliability and Cronbach's alpha values above these thresholds, confirming their internal reliability and consistency.

4.2.4 Convergent validity

For determining the average variance extracted (AVE) as a part of the assessment of convergent validity. A minimum of 0.50 is required for acceptable validity. (Sultana & Akter, 2025). Table 4.2 illustrates that all constructions have convergent validity and AVE values above the 0.50 criterion.

4.2.5 Discriminant Validity

Table 4.3: Fornell-Larcker Criterion

FORNELL	AU	Age group	BI	PEOU	PU	SPR
AU	0.923					
Age group	-0.344	1				
BI	0.869	-0.331	0.916			
PEOU	0.84	-0.408	0.845	0.923		
PU	0.833	-0.392	0.833	0.881	0.923	
SPR	0.38	-0.1	0.412	0.354	0.329	0.927

Source: Author's own data analysis from SmartPLS.

Table 4.4: Heterotrait Monotrait ratio (HTMT)

HTMT	AU	Age group	BI	PEOU	PU	SPR
AU						
Age group	0.352					
BI	**0.910**	0.34				
PEOU	0.878	0.418	0.885			
PU	0.871	0.401	0.872	**0.921**		
SPR	0.395	0.101	0.429	0.368	0.342	

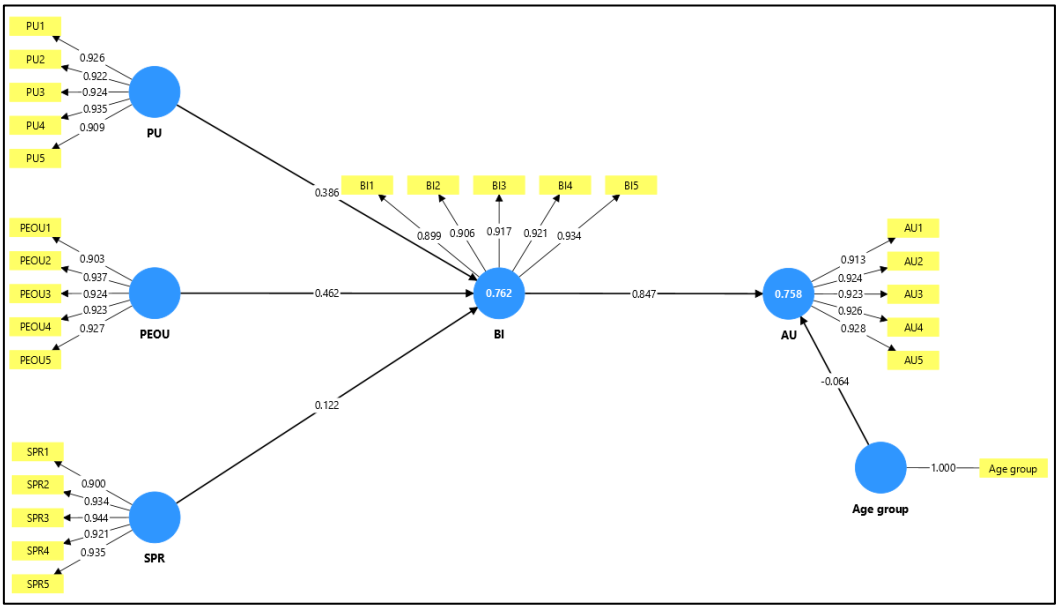
Source: Author's own data analysis from SmartPLS.

The purpose of assessing discriminant validity is to avoid multicollinearity. The Heterotrait-Monotrait (HTMT) ratio represents a more recent approach, although the Fornell-Larcker criterion remains the most widely utilized method (Ab Hamid et al., 2017). Tables 4.3 and 4.4 present the results of the current study using both methods. Moreover, the control variable (age group) was treated as a single-indicator construct and therefore included in the measurement model assessment; however, this does not influence the main TAM relationships. Discriminate validity is achieved when the square root of a construct's AVE is greater than its correlations with other constructs. As shown in Table 4.3, all constructions fully satisfied this requirement. For the second approach, most HTMT values were below the conservative threshold of 0.85, while 0.90 represents a more liberal cut-off (Ab Hamid et al., 2017). Cros Overall, Table 4.4 met the HTMT requirement acceptably.

4.2.6 Structural Model Assessment

In the second stage of model evaluation, the structural model was assessed to examine the predictive relationships among the latent constructs. This assessment included evaluating the overall model fit (SRMR), checking multicollinearity through VIF values, and determining the explanatory power of the model using R^2. The predictive relevance was further assessed using Q^2, while effect sizes (f^2) were examined to determine the strength of each predictor. In addition, the significance of the hypothesised paths was evaluated using the standardised path coefficients (β), t-values and p-values generated through the bootstrapping procedure.

Figure 4.2: Structural model PLS results



Source: Author's own data analysis from SmartPLS.

Table 4.5: Coefficients of Determination (R^2)

Constructs	R-square	R-square adjusted
AU	0.758	0.756
BI	0.762	0.76

Source: Author's own data analysis from SmartPLS.

The structural model's explanatory power was evaluated using the coefficient of determination (R^2) (Hair et al., 2021; Pereira et al., 2024). According to Chin (1998), R^2 values of 0.19, 0.33, and 0.67 indicate weak, moderate, and high levels of explanatory power in PLS path models, respectively. As shown in Figure 4.1 and Table 4.5, the R^2 value for behavioral intention (BI) is 0.762, indicating that PU, PEOU, and SPR collectively explain 76.2% of the variance in BI. This demonstrates that the three predictors have a strong influence on users' intention to adopt biometric authentication.

Similarly, the R^2 value for actual usage (AU) is 0.758, suggesting that BI and the control variable (age group) explain 75.8% of the variance in AU. Based on Chin's (1998) guideline, this also reflects substantial explanatory power, indicating that the structural model predicts actual biometric authentication usage effectively.

Table 4.6: Model fit summary

	Saturated model	**Estimated model**
SRMR	0.031	0.045
d_ULS	0.34	0.715
d_G	0.557	0.599
Chi-square	1008.758	1065.969
NFI	0.908	0.903

Source: Author's own data analysis from SmartPLS.

Table 4.7: Main Effects and Path Coefficients

Hypotheses	**Paths**	**Beta (β)**	**Standard deviation**	**t-value**	**p-value**	**Variance Inflation Factor (VIF)**	**f^2**	**Decision**	**Relationship**
H1	PU → BI	0.386	0.063	6.086	0.000	4.479	0.140	Support	Positive
H2	PEOU → BI	0.462	0.062	7.416	0.000	4.565	0.197	Support	Positive
H3	SPR → BI	0.122	0.029	4.159	0.000	1.145	0.054	Support	Positive
H4	BI → AU	0.847	0.022	39.295	0.000	1.123	2.642	Support	Strong positive

** P-value less than 0.05 or 5% considered as significant*

Source: Author's own data analysis from SmartPLS.

For this research, the equation is shown below:

$$Y = \alpha + 0.386PU + 0.462PEOU + 0.122SPR + 0.847BI + \in$$

Whereby,

Y = Actual Use Behavour

PU= Perceived Usefulness

PEOU= Perceived Ease of Use

SPR= Security and Privacy Risks

BI= Behavioral intention to adopt biometric authentication

Table 4.6 summarizes the model fit summary generated from SmartPLS, including the SRMR, d_ULS, d_G, Chi-square, and Normed Fit Index (NFI).

According to Henseler et al. (2016), indicated SRMR score lower than 0.08 suggests an appropriate model fit. In this study, both the saturated model (SRMR = 0.031) and the estimated model (SRMR = 0.045) meet this standard, indicating a good model fit to the data. The NFI values are 0.908 (saturated model) and 0.903 (estimated model), both exceed the benchmark of 0.90, providing further evidence of good model fit (Sultana & Akter, 2025). Overall, these findings confirm that the model well represents the data structure and is consistent with the theoretical framework.

Table 4.7 summarizes the results of the structural model such as the path coefficients, standard deviations, t-values, p-values, variance inflation factor (VIF), and effect sizes (f^2). The significance of all structural paths was evaluated using the bootstrapping procedure. According to Hair et al. (2021), result the path is considered statistically significant when the t-value is greater than 1.96 and p is less than 0.05. As shown in Table 4.7, all hypothesized relationships meet this criterion. PU showed a significant effect on BI， which result are (β = 0.386, t-value = 6.086, p < 0.001), supporting H1. This reflects a **positive relationship**, suggesting that higher perceived ease of use leads to stronger behavioural intention. Similarly, PEOU exerts a strong and significant effect on BI, which results are shows (β = 0.462, t-value = 7.416, p < 0.001), supporting H2. This reflects a **positive relationship**, suggesting that higher perceived ease of use leads to stronger behavioural intention. Moreover, SPR also have a positive impact on BI, which result are shows (β = 0.122, t-value = 4.159, p < 0.001), supporting H3. Although the relationship is **positive**, the relatively smaller coefficient indicates a **weaker positive relationship** compared to PU and PEOU.These findings are consistent with previous TAM-based research, in which PU, PEOU, and risk-related structures are often important predictors of intent. Behavioral intention strongly predicts actual usage (AU), with a substantial path coefficient (β = 0.847) and a very high t-value (39.295), providing strong support for H4. This demonstrates a **strong positive relationship** between behavioural intention and actual usage.

The variance inflation factor (VIF) values for all paths were below the recommended threshold of 3.3, confirming that there is no multicollinearity (Kock,

2015). Effect size analysis (f^2) benchmarks, where 0.02,0.15 and 0.35 represent small, medium, and large effects respectively (Cohen, 1988). The effect of BI on AU shows a large effect (f^2 = 2.642), while PU → BI (f^2= 0.14) and PEOU → BI (f^2 = 0.197) indicate medium effects. SPR → BI (f^2 = 0.054) represents a small effect. These results support the corresponding R^2 values of the model, further confirming its strong explanatory power. Overall, all hypotheses (H1–H4) are supported. The model demonstrates strong predictive validity, satisfactory model fit, and no multicollinearity issues, confirming the robustness of the structural model.

4.2.7 Predictive Model

Table 4.8: Result of Predictive Model

	Q^2predict
AU	0.732
BI	0.759

Source: Author's own data analysis from SmartPLS.

The results indicate that the predictive model effectively assesses the relevance and predictive characteristics of the study. According to PLS predict guidelines (Shmueli et al., 2016), the Q^2 value must be greater than zero to demonstrate meaningful predictive relevance for the training or holdout samples. As shown in Table X, both constructs recorded positive Q^2predict values, with BI = 0.759 and AU = 0.732, which exceed the minimum requirement. Therefore, these results confirm that the model exhibits satisfactory out-of-sample predictive performance, demonstrating that the PLS path model can generate accurate predictions for behavioral intention and actual usage behavior.

4.3 Bootstrapping Results by Age Group (Control Variable)

This section examines age-based differences in behavioural responses to biometric authentication by dividing respondents into three groups: youth (28 years and under), middle-aged (29-60 years), and elderly (61 years and over). The SmartPLS bootstrapping procedure was applied separately to each age group to estimate the structural model. The analysis focused on path coefficients (β), t-statistics, and p-values to assess the statistical significance of the hypothesized relationships (Ali, 2022).

4.3.1 Young Age Group

Table 4.9: Young Age Group (28 years and under)

Hypotheses	Paths	Beta (β)	T-Statistics	P-value	Result	Relationship
H1	PU -> BI	0.559	24.941	0.000	Support*	Positive
H2	PEOU -> BI	0.299	2.082	0.037	Support*	Positive
H3	SPR -> BI	0.045	3.763	0.000	Support*	Positive
H4	BI -> AU	0.859	0.996	0.320	Not Support	Positive (Not Significant)

Note: *Relationship is significant at P < 0.05

Source: Author's own data analysis from SmartPLS.

Among the young age groups, the results show that PU has the strongest significant effect on BI ($\beta = 0.559$, $p < 0.000$), indicating that younger respondents are mainly motivated by the perceived benefits of biometric authentication. Although PEOU ($\beta = 0.299$, $p = 0.037$) and SPR ($\beta = 0.045$, $p < 0.000$) also significantly predict BI, their effects are comparatively smaller. Importantly, BI does not significantly influence AU ($\beta = 0.859$, $p = 0.320$), indicating that a gap between intention and behavior, meaning that young people express a willingness to use biometric technology, but may not necessarily translate that willingness into actual use.

4.3.2 Middle Aged Group

Table 4.10: Middle Age Group (29 - 60 years)

Hypotheses	Paths	Beta (β)	T-Statistics	P-value	Result	Relationship
H1	PU -> BI	0.428	3.530	0.000	Support*	Positive
H2	PEOU -> BI	0.418	3.418	0.001	Support*	Positive
H3	SPR -> BI	0.126	2.627	0.009	Support*	Positive
H4	BI -> AU	0.896	37.72	0.000	Support*	Strong Positive

Note: *Relationship is significant at P < 0.05

Source: Author's own data analysis from SmartPLS.

In contrast, middle-aged adults show all relationships are significant, with PU (β = 0.428, p < 0.000) and PEOU (β = 0.418, p = 0.001) showing relatively balanced effects on BI. SPR also remains meaningful (β = 0.126, p = 0.009), indicating moderate sensitivity to security concerns. This group exhibited the strongest relationship between behavioural intention and actual use show (β = 0.896, p < 0.000), suggesting their behavior is highly consistent and that middle-aged users are able to reliably translate intention into actual use.

4.3.3 Older Aged Group

Table 4.11: Older Age Group (61 years and over)

Hypotheses	Paths	Beta (β)	T-Statistics	P-value	Result	Relationship
H1	PU -> BI	0.293	3.364	0.001	Support*	Positive
H2	PEOU -> BI	0.518	6.228	0.000	Support*	Positive
H3	SPR -> BI	0.198	2.851	0.004	Support*	Positive
H4	BI -> AU	0.812	20.657	0.000	Support*	Strong Positive

Note: *Relationship is significant at P < 0.05

Source: Author's own data analysis from SmartPLS.

For the older adult group, PU shows the weakest influence on behavioural intention (β = 0.293, p = 0.001), while PEOU becomes the most dominant predictor of BI (β = 0.518, p < 0.001). This indicates that older users place substantial emphasis on simplicity and ease of operation when considering biometric authentication. Security and privacy risks (SPR) also exhibit a stronger influence in this group (β = 0.198, p = 0.004), reflecting heightened sensitivity to security and privacy concerns. Similar to the middle-aged group, behavioural intention significantly predicts actual usage (AU) (β = 0.812, p < 0.001), indicating stable adoption behaviour once intention is formed.

4.3.4 Summary of Age-Based Differences

Overall, the findings show clear differences across age groups. Young adults are primarily influenced by how useful biometrics seem to them, but they often do not turn this intention into real usage. Middle-aged adults demonstrate the most steady and reliable adoption behavior, as their intention strongly leads to actual behavior. Older adults are more care about ease of use and are more cautious about security, but once they decide to use biometrics, they follow through and use it consistently.

4.4 Conclusion

This section analyzed the data collected through descriptive analysis, measurement model assessment, and structural model analysis in SmartPLS 4.0. Descriptive analysis summarized respondents' demographic data, such as age, gender, and education level. The measurement model evaluation showed satisfactory indicator reliability, internal consistency, convergent validity, and discriminant validity. The structural model study looked at collinear and path links between the constructions. Results show that perceived value, perceived ease of use, and concerns about

privacy and security each have an important effect on behavioral intention, while behavioral intention predicts actual use of biometric authentication. Age, as considered a control variable, has a statistically significant impact on actual usage behavior.

CHAPTER 5: DISCUSSION, CONCLUSION, AND IMPLICATIONS

5.0 Introduction

This section includes the findings of this study based on the survey data that were analyzed in the previous section. This section covers the study's significant findings based on the survey data analyzed in the previous section. Besides, the study also acknowledges its limitations and provides suggestions for future research so that it can give helpful directions for further investigation. Finally, this chapter also provides an overall summary of the whole research.

5.1 Summary of Statistical Analysis

This section highlights the descriptive and inferential analysis carried out on the research data. Based on the data collected from 324 respondents. The respondents consisted of Malaysian citizens ranging from Generation Z to the Silent Generation, with ages from below 28 to above 80. When filtering the collected information, 300 sets of questionnaires were utilized in the analysis. The analysis provides insight into the information in the database by studying the characteristics of the different variables and revealing the most important trends and correlations within the dataset.

5.1.1 Summary of Descriptive Analysis

In the study, 54.3% of the responses were provided by female participants, while only 45.7% of the answers came from male participants. Most of the respondents are aged 28 or below (35.3%), followed by those aged 61–79 (24.7%). The proportions in the age groups of 45-60 (17.3%), 29-44 (16.3%), and 80 and above

(6.3%) were relatively small. In this research study, female respondents contributed 163 persons (54.3%) of the entire sample, with males accounting for the remaining 137 persons (45.7%). Most of the respondents are aged 28 or below (35.3%), followed by those aged 61–79 (24.7%). The proportions in the age groups of 45-60 (17.3%), 29-44 (16.3%), and 80 and above (6.3%) were relatively small. Most people surveyed had a bachelor's degree (42.3%); the next highest percentage completed Secondary Certificates (34.3%), SPM, or UEC. Diploma holders represent 15.3% of the sample, while 4.3% of the sample possessed a master's degree or higher, and 3.7% possessed a Foundation Certificate. The results provide information about the personal characteristics of the sample, which allows us to better understand the characteristics of our target population and how these characteristics impact their willingness to adopt biometric authentication, based on age group and location in Malaysia.

5.1.2 Summary Statistical Analysis

The statistical analysis based on 300 valid responses indicates that SPR exhibits the highest level of internal consistency, as reflected by Cronbach's alpha and composite reliability values, followed by PU, PEOU, AU, and BI. All constructs' AVE values are greater than threshold of 0.50, revealing their convergent validity.

Furthermore, the study model demonstrates discriminant validity, confirmed by the Fornell-Larcker Criterion, and HTMT results. Although the HTMT results show two pairs (BI - AU and PEOU - PU) slightly exceeded 0.90 correlations which (0.910 and 0.921). These higher correlations are expected in TAM-based studies and do not affect the validity of the measurement model. In terms of path coefficients, PU, PEOU, and SPR significantly impact BI, with BI and AU showing had strong significant relationship. The p-value and path coefficient results indicate that PU, PEOU, and SPR significantly influence behavioral intention, while behavioral intention significantly predicts actual usage. The Predictive Model has shown to perform satisfactorily. Its predictive relevance to both behavior intention

(BI) and actual usage (AU) is high as reflected by the Q-squared values of both BI and AU. Ranked in terms of the size of each variable's effect size (ES) on the BI and AU, BI has the largest ES on AU. PEOU and PU contribute ES to the BI, while SPR has much less influence on BI's PQ. In additional age was included as a control variable, and age-based bootstrapping analysis reveals variations in the strength of relationships across age groups. Younger users show a weaker translation of behavioral intention into actual usage, while middle-aged and older users demonstrate more consistent adoption behavior.

Table 5.1: Summary of Bootstrapping result

Variable	Result (p-value)	Significance level	Result Consistency with Expected Sign
PU → BI	0.000***	Highly significant	Consistent
PEOU → BI	0.000***	Highly significant	Consistent
SPR → BI	0.000***	Highly significant	Consistent
BI → AU	0.000***	Highly significant	Consistent

Note: ***, **, * denote significance at 1%, 5%, and 10% levels respectively.

Source: Developed by the authors

5.2 Discussion on Major Findings

5.2.1 Perceived Usefulness (PU)

RQ1: What is the effect of Perceived Usefulness (PU) on consumers' behavioural intention to adopt biometric authentication?

RO1: To identify the effect of Perceived Usefulness (PU) on consumers' behavioral intention to adopt biometric authentication.

H1: Perceived Usefulness (PU) has a significant influence effect on consumers' behavioral intention to adopt biometric authentication.

Perceived Usefulness (PU) is important for the user to decide on adopting Biometric Authentication. From our data, we can say that PU is significantly related to the users' behavioral intentions when using Biometric Authentication as well as helps establish Hypothesis #1 as Supported. Users view Biometric Authentication as a method of securing digital transactions with greater levels of Efficiency & Convenience than current forms of authentication; they tend to express stronger intentions to adopt these methods than others. The Technology Acceptance Model (TAM) outlines that users' behavioral intentions to accept using Technology are heavily influenced by a perception about the usefulness of the Technology (PU). Based on the findings of Rukhiran et al. (2023), users will be more likely to use a Biometric System to improve authentication accuracy, increase speed of identification, increase reliability and security, and reduce risk of unauthorized access. This finding is also consistent with many previous studies that have found PU to be one of the most significant variables influencing users' intentions to adopt biometric-based systems, especially in applications related to Financial Security and/or Security-Sensitive Areas (Piotrowska, 2024)

5.2.2 Perceived Ease of Use (PEOU)

RQ2: How does Perceived Ease of Use (PEOU) influence consumers' behavioural intention to adopt biometric authentication?
RO2: To investigate the effect of Perceived Ease of Use (PEOU) on consumers' behavioral intention to adopt biometric authentication.
H2: Perceived Ease of Use (PEOU) has a significant influence on consumers' behavioral intention to adopt biometric authentication.

The hypothesis test demonstrates that perceived ease of use (PEOU) has a strong and significant effect on behavioral intention to adopt biometric authentication. This indicates that when biometric systems are easy to learn, understand, and operate, consumers are more likely to develop a stronger intention to adopt such technologies.

This finding is consistent with the Technology Acceptance Model (TAM), which posits that perceived ease of use directly influences behavioral intention. In the context of biometric authentication, systems that require minimal effort and involve low operational complexity reduce users' cognitive burden and enhance convenience during authentication. This is supported by Kruzikova et al., (2022), study found that fingerprint authentication is perceived as highly usable because it is fast, requires no additional device, and involves low complexity. The findings further show that fingerprint verification was evaluated as the most usable method by both younger (26 - 54) and older users (55 and above), indicating that simplified biometric systems are particularly suitable for older age groups.

Consistent with prior empirical studies, perceived ease of use demonstrates a positive effect on consumers' intention to adopt biometric technologies, particularly in applications such as mobile banking and digital payments (Wang, 2021; Piotrowska, 2024). Overall, these findings highlight the importance of designing biometric authentication systems that are simple and intuitive to promote adoption intention.

5.2.3 Security and Privacy Risks (SPR)

RQ3: What Security and Privacy Risks affect consumers' behavioural intention to adopt biometric authentication?
RO3: To evaluate the influence of Security and Privacy Risks (SPR) on consumers' behavioral intention to adopt biometric authentication.
H3: Security and Privacy Risks (SPR) have a significant influence effect on consumers' behavioral intention to adopt biometric authentication.

The results show that SPR has a significant influence on consumers' behavioral intention to adopt biometric authentication. This finding suggests that security and privacy considerations play an important role in shaping users' adoption decisions with the intention of adopting biometric systems.

Previous studies have reported mixed findings (negative or positive relationship) regarding the effect of security and privacy risks on behavioral intention. The research performed by Nan et al. (2022) illustrates how users may have a diminished desire to adopt biometric systems due to an individual's perception of that technology being vulnerable. However, this contrarily may be the case for an increase in an individual's intention to adopt biometric systems when they perceive a greater level of security than that provided by traditional authentication methods (Wirawan & Utomo, 2024). Therefore, these studies show that the security and privacy concerns surrounding a specific biometric system are largely based on the circumstances surrounding the user. In the framework of the study, the significant influence of SPR may be explained by users' perception of biometric authentication as a protective mechanism rather than a source of risk. As biometric systems are commonly associated with enhanced protection against identity theft, fraud, and unauthorized access, greater awareness of security and privacy issues may motivate consumers to adopt biometric authentication as a preventive solution. This interpretation is consistent with Stylios et al. (2022), who suggest that security awareness can enhance perceived usefulness when biometric technologies are seen as effective in safeguarding personal data.

Based on the empirical results of this study, SPR have a positive impact on behavioral intentions, indicating that when users perceive biometric authentication systems as secure and reliable, those who are more concerned about security and privacy are more likely to have a stronger willingness to adopt them.

5.2.4 Behavioural Intention (BI)

RQ4: What is the relationship between consumers' behavioural intention and their actual use behaviour of biometric authentication?

RO4: To evaluate the relationship between behavioral intention and actual use behavior of biometric authentication.

H4: Behavioral intention to adopt biometric authentication has a significant effect on actual usage behavior.

The hypothesis testing results indicate that BI has a significant influence on consumers' actual usage behavior of biometric authentication. These results show that the adopting intention of consumers towards biometric authentication are very important while it comes to determining whether intention is translated into actual system use.

This result is consistent with the TAM, which posits that behavioral intention is the most direct antecedent of actual usage behavior.According to Kumalasari et al. (2024), behavioral intention has the most significant influence on use behavior and is considered a direct antecedent of actual behavior in biometric-based self-service technology. Users that have a strong intention to adopt biometric authentication are more inclined to use biometric authentication for mobile banking, sending money digitally, and logging into systems on a regular basis in their daily use of digital activity.

The strong relationship between perceived behavioral intentions and actual use of biometric systems found in this research is consistent with existing research on the same topic. Existing research has consistently demonstrated that people's perceived behavioral intentions are the most significant predictors of how often they will use biometric authentication systems and have been shown in various settings, including Education, Healthcare, and Financial Services (Rukhiran et al., 2023; Fitrianie et al., 2021; Wirawan & Utomo, 2024).

Additionally, all the research studies previously discussed indicate that once an individual establishes a strong intention to use biometrics, then that individual will continue to have a high probability of using biometric technology consistently.

For the purposes of this research, establishing a strong positive correlation between perceived behavioral intention and actual usage behaviour provides additional evidence that a strong intention is an important mechanism for converting perceptual and attitudinal factors into real-world adoption of biometric authentication technologies.

5.2.5 Age as Control Variable

RQ5: How does controlling for age help ensure unbiased analysis of consumers' actual usage behavior of biometric authentication?
RO5: To control for age in the analysis of actual usage behavior, ensuring that demographic differences do not bias the final behavioral outcomes.

The results show that there are significant differences in usage patterns among users of different age groups. According to young users, PU, PEOU, and SPR may lead users to intend to use biometric authentication systems, this does not mean that BI and AU have a significant impact. Previous research on the intention-behavior gap has shown that when user attitude strength is weak or personal relevance is low, indicated that intention alone is often not enough to lead to actual behavior (Bhattacherjee & Sanford, 2009).For younger users, biometric authentication may be perceived as convenient rather than necessary, resulting in lower commitment and an insignificant BI and AU relationship.

In contrast, middle-aged users demonstrate the most consistent adoption behavior, with behavioral intention showing a strong and significant influence on actual usage. This result indicates that intention among middle-aged users is more effectively translated into real behavior. According to Kusairi et al. (2025), the study explains that when users have enough experience, resources, and support are more likely to turn their intention into real usage behavior. Middle-aged users are found to be more likely to complete their routine activities by relying on biometric authentication than younger users, such as mobile banking and digital payments, which reduces the intention-behavior gap and results in more stable adoption behavior.

Research indicates that, when compared to younger users, older users have a greater concern for how easy something will be to use (or find) and for security and privacy concerns. The results from Gao et al. (2025) support this finding as older users are less likely to continue using systems that use biometrics like facial

recognition on making payments and shopping online because they perceive more uncertainty and risk associated with these payment methods.

Overall, demographic groups demonstrate different patterns related to the adoption of new technologies and the usage of these technologies over time. Consequently, age should be controlled for in the analysis to illustrate that differences between groups in actual usage behavior may occur as a result of other demographic variables. This helps in supporting the RQ5 and RO5 in the research.

5.3 Implication of Study

5.3.1 Theoretical Implications

From an academic perspective, the Technology Acceptance Model (TAM) is utilized in the context of biometric authentication in Malaysia in this study, ensuring a contribution to the technology adoption literature. However, there are still only a small number of studies that apply the TAM to specifically explain biometric authentication, although TAM has been widely used to explain the adoption of various digital technologies. According to Lancelot Miltgen et al. (2013), only a few authors have discussed biometric systems from a consumer acceptance perspective. Moreover, according to Domingo et al. (2025), biometric systems such as fingerprint and face recognition have come up in this regard, but palm biometric systems are still underexplored. Therefore, this study tends to provide empirical support so that the applicability of TAM can be proved in a security-sensitive authentication context. However, there are serious issues about privacy and security of biometric information. (Domingo et al., 2025). Besides, the existence of security and privacy risks also helps in extending the traditional TAM framework by incorporating risk-related concerns that relate to biometric technologies. By examining both behavioural intention and actual usage behaviour, this study also contributes to the literature by addressing the intention–behaviour gap that is often overlooked in technology adoption research. Overall, the findings offer a concise

theoretical contribution that can serve as a reference for future studies on biometric authentication adoption.

5.3.2 Practical Implications

5.3.2.1 Practical Implications for Government

By conducting this study, policymakers will gain more crucial insights into the factors that influence consumers' adoption of biometric authentication in digital financial and online service environments. Several findings have proved that privacy protection perception of users and data security play a crucial role in influencing their adoption intention. Concerns regarding user privacy and security are a major barrier preventing people from using biometric authentication technology. Users need to understand the ways in which their biometric information will be collected, stored, accessed, and utilized by the company that develops the biometric authentication technology (Zihan Kalila Gusnan & Rio Guntur Utomo, 2024). This shows there are additional reasons for companies to implement biometric authentication technologies; that is, it is equally important for users to feel secure about how the biometric information will be protected. Privacy and security are key obstacles to greater use of biometric authentication (Zihan Kalila Gusnan & Rio Guntur Utomo, 2024). However, because of face immutability, security is a problem that people pay close attention to, and leakage of personal information harms people's faith in face recognition technology (Zhang, 2024). These findings potentially help policymakers to get more understand about the importance of regulatory assurance while shaping public trust toward biometric technologies. The concern regarding the issue of unauthorized access to biometrics as well as data misuse and the long-term retention of biometric information, all highlight the need for a transparent, well-defined governance framework surrounding biometric use. As stated by Zhang (2024), how the general public perceives a loss of privacy is one of the greatest issues facing the use of biometrics today. In fact, relevant sectors, such as digital banking, e-wallet services, and

government-linked digital identity systems, really need those insights since their biometric authentication is increasingly implemented.

Thus, policymakers should give some consideration to strengthening the old policies and guidelines related to biometric data governance. For instance, to prevent uncertainty and possible risks among users, the standards can be established clearly regarding the collection, storage, processing, and deletion of biometric data. Moreover, policymakers can also increase the users' confidence in biometric authentication systems by providing regulatory measures that help in emphasizing accountability and data protection responsibilities. By doing these, a more trusted and user-oriented digital ecosystem can be provided to the users because the biometric authentication technologies are adopted responsibly. This potentially assists in encouraging more people to accept biometric authentication.

5.3.2.2 Practical Implications for Practitioners (FinTech Firms and Biometric System Developers)

The practical implications of this section play a crucial role in understanding the major factors that make consumers accept the biometric authentication systems for characters like FinTech companies, system designers, and developers of biometric authentication. Consumer acceptance of biometric authentication technology is significantly influenced by Perceived Usefulness (PU) as well as Perceived Ease of Use (PEOU) (Stylios et al.,2022). Therefore, in order to increase the likelihood that consumers will accept a biometric authentication system as an alternative to traditional authentication methods, practitioners must develop biometric authentication systems that provide users with easily understood functional value propositions (Erwin et al.,2025). Systems that fulfil the day-to-day requirements of consumers, such as faster access to funds, greater convenience and security, and improved accuracy, will provide powerful incentives to adopt biometric authentication solutions. For instance, the inclusion of biometric authentication options on mobile payments and banking services allows consumers to process transactions quickly and securely using either their fingerprint or facial

recognition. This reduces the number of steps for users, lowers the authentication error rate, and maximizes accuracy and ease of use.

From a practical perspective, a simple and intuitive user interface design is crucial for improving perceived ease of use and the overall user experience. According to Cheng (2025) highlighted that well-designed interface and intuitive navigation enhance usability, reduce cognitive burden, and strengthen consumer motivation in mobile banking applications. Besides, this also assists in providing smoother interactions and faster transactions, indicating improvement of system performance, decrease of user errors, and reliance on customer service. For instance, if a user forgets their password, they need to contact customer service for help. Besides, the number of redundant or inactive accounts can be successfully minimized since the user abandonment caused by forgotten passwords is reduced, and the unnecessary creation of new accounts is prevented. Overall, Biometric authentication enhances user acceptance of these systems, encourages users to use them consistently and stably, and ultimately becomes a loyal user and system performance well for practitioners.

5.3.2.3 Practical Implications for Consumers

Based on the findings, consumers' decisions to use a technological feature (biometric system) are influenced by factors such as convenience, ease of use, and perceived security and privacy risks. Therefore, consumers should evaluate biometric authentication not only in terms of PU and PEOU but also consider data protection practices and control over personal information (Stylios et al., 2022).In addition, when biometric systems not only minimize challenges with authenticating users but also enhance the efficiency of transactions while safeguarding personal information and providing security, they enable consumers to evaluate their own behaviour and make informed and responsible choices regarding how they use a service(s).

As an example, by having access to biometric validation methods through mobile banking and/or digital wallets, consumers are able to determine whether the implementation of fingerprint recognition or facial recognition enhances their access to a service at a far greater rate than traditional passwords have provided. On the other hand, consumers also need to review consent settings, data storage policies, and recovery options in case of authentication failure. Biometric authentication may be viewed as more easily utilized and secure when compared to traditional password systems; however, once attacked, the biometrics cannot be changed, and thus privacy protection and educated consent must be part of responsible biometric use (Piotrowska 2024, Rukhiran et al. 2023).

In particular, for elderly users, effective use of biometric authentication requires certain conveniences, such as assistance from a family member, clear in-app instructions, and access to alternative services. These convenience features mitigate some aspects of physiological and cognitive bias associated with aging and thus reduce complications of using biometric systems (Kumalasari et al. 2024). Through this approach, consumers can develop trust in the use of biometric authentication while also more effectively addressing security and privacy concerns, which they may have, and therefore allow the consumer to safely and securely integrate biometric technology into their daily digital lives.

5.4 Limitations of the Study

Although this research provides new information about the forces behind why people in Malaysia may become interested in using biometrics for authentication purposes, there are also some limitations relevant to this study. First of all, this study utilized cross-sectional research methods and therefore took a single snapshot of people's attitudes; it does not address the changing nature of people's attitudes toward using biometrics for authentication, as development and usage patterns of biometric technologies increase. Additionally, whilst age was considered only as a demographic variable and not as a potential mediator of the study's findings, this aspect could have considerable effects on consumer behavior

towards the adoption of biometric Authentication systems. This choice helps reduce demographic bias in behavioral outcomes, but it also limits the ability to explore the psychological factors that could affect decision-making at different ages.

Another limitation of this study is the uneven age distribution of respondents. Although participants ranged from under 28 to over 80, most were 28 years and under (35.3%) or 61-79 years (24.7%). Those 80 and over made up only a small fraction (6.3%). This imbalance is mainly due to practical limitations. The oldest group was harder to reach, and some groups had difficulties with literacy or digital skills, which limited their ability to complete the questionnaire. Therefore, the findings mainly represent elderly users with basic digital literacy and prior biometric experience.

Finally, this study is subject to limitations related to the applicability of certain biometric authentication methods. Some users might find that fingerprint and facial recognition may not be very effective for them due to several factors, such as fingerprint wear or blurring, physical injury, or facial changes. Although these users represent a minority, and other authentication methods are usually available, biometric authentication is not perfect and may not be suitable for all users. According to Zhao et al. (2021), fingerprint recognition is affected by fingerprint damage, dirt, moisture, and skin condition, while facial recognition accuracy decreases due to changes in facial appearance, lighting, posture, and facial expressions. This can affect the acceptance and ease of use of biometric technologies by specific groups.

5.5 Recommendations for Future Research

While the scope of this study considers age as a variable of interest in its analysis of biometric authentication, future studies could benefit from a wider range of age categories that reflect how demographic differences exist within Malaysia. Although this study utilised the commonly used age categories found in existing literature, researchers may wish to consider developing other age groupings for

Malaysian audiences, such as Generation Z (18-40 years) and Generation X (41-60 years), as well as Baby Boomers and Silent Generation (61-90 years). These alternate groupings could lead to more comprehensive analysis regarding the impact of generational identity, socio-economic status, technology, etc., on biometric authentication, and provide opportunities for comparing generational differences based upon their stage in life.

Furthermore, future research could examine age as a moderating variable rather than a control variable. While controlling for age reduces demographic bias, it does not fully enough to define differences groups in intention to adopt biometric authentication. According to previous study had shown that age be moderates a key relationship in the TAM, to impact of PU and PEOU on BI, with a stronger effect in older users (Faqih, 2015). As including age as a moderating variable would provide a deeper understanding of biomarker across age group.

Moreover, for methodological part in future research should apply Multi-Group Analysis (MGA) using PLS-SEM to compare structural relationships across age groups. MGA allows researchers to assess differences across two or more subgroups (Cheah et al., 2020). This helps gain deeper insights into whether key determinants and technology adoption behaviour have different impacts on users of different ages.

Finally, incorporating qualitative research methods, such as combining quantitative surveys with qualitative interviews. Although survey data can provide generalizable findings, additional interviews can offer a deeper understanding of users' personal experiences, challenges, and coping strategies when using biometric authentication for each group.

5.6 Conclusion

In conclusion, this study has investigated key factors influencing consumers' behavioural intention and actual usage of biometric authentication in Malaysia by applying the Technology Acceptance Model (TAM) and extending it with security

and privacy risks, while controlling for age to minimise demographic bias. All the research objectives were successfully achieved, and the findings provide meaningful theoretical and practical insights into biometric authentication adoption.

These results have broad consequences for various sectors, including government, the Practitioners and the consumer who use biometric authentication. For the government, it is vital to develop and maintain regulatory safeguards and privacy protections related to the use of biometric data, as well as publicly transparent governance over the use of biometric data to gain and maintain the trust of consumers. The Malaysian government should use the findings from this study to support the recommendation and implementation of Biometric Authentication as a method for consumer verification; implement regulation of the Biometric Authentication Industry; and improve public awareness of how the Biometric Authentication Ecosystem works, which will assist in building the public's trust and increase the perceived advantage of the Biometric Authentication Ecosystem.

Fintech Innovators and Biometric Authentication System Developers can use the advantages of Biometric Authentication as a method to both attract and retain Users by utilizing Biometric Authentication's ability to minimize the potential for Cyber-Attacks and Provide Data Privacy. In addition to protecting personal details for Consumers, it is critical that privacy awareness is created and ample support for Security is provided to Older Consumers.

Despite the many topics studied, there are several limitations of the current study, including the Cross-sectional Study Design, the uneven distribution of age groups, and the limitations of some Biometric Modalities to certain age and user groups. Addressing these limitations for further Research will provide Comprehensive Knowledge of the factors that affect Consumer Intention to adopt Biometric Authentication Across All Ages in Malaysia.

REFERENCES

Abdullah, N., Redzuan, F., & Daud, N. A. (2020). E-wallet: Factors influencing user acceptance towards cashless society in Malaysia among public universities. *Indonesian Journal of Electrical Engineering and Computer Science, 20*(1), 67–74. https://doi.org/10.11591/ijeecs.v20.i1.pp67-74-67

Ab Hamid, M. R., Sami, W., & Mohmad Sidek, M. H. (2017). Discriminant validity assessment: Use of Fornell & Larcker criterion versus HTMT criterion. *Journal of Physics: Conference Series, 890*, 012163. https://doi.org/10.1088/1742-6596/890/1/012163

Ajayi, V. O. (2023). A review on primary sources of data and secondary sources of data. *Universal Journal of Arts, Humanities, Science and Technology Education Research (UJAHSTER), 2*(3), 1–3. https://doi.org/10.5281/zenodo.16739602

Ali, Q., Parveen, S., Yaacob, H., & Zaini, Z. (2021). Cardless banking system in Malaysia: An extended TAM. *Risks, 9*(2), 41. https://doi.org/10.3390/risks9020041

Ali Saare, M., Hussain, A., & Seng Yue, W. (2019). Conceptualizing mobile health application use intention and adoption among Iraqian older adults: From the perspective of expanded technology acceptance model. *International Journal of Interactive Mobile Technologies (iJIM), 13*(10), 28. https://doi.org/10.3991/ijim.v13i10.11285

Allanson, P. E., & Notar, C. E. (2020). Statistics as measurement: 4 scales/levels of measurement. Education Quarterly https://doi.org/10.31014/aior.1993.03.03.146

Amini, M., & Javidnejad, L. (2024). Legal regulation of biometric data: A comparative analysis of global standards. *Legal Studies in Digital Age, 3*(1), 26–34.

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist, 37*(2), 122.

Bhardwaj, P. (2019). Types of sampling in research. *Journal of the Practice of Cardiovascular Sciences, 5*(3), 157. https://doi.org/10.4103/jpcs.jpcs_62_19

Bhattacherjee, A., & Sanford, C. (2009). The intention–behaviour gap in technology usage: The moderating role of Attitude Strength. *Behaviour*

& Information Technology, *28*(4), 389–401. https://doi.org/10.1080/01449290802121230

Binbeshr, F. S. S. (2022). *A secure PIN-entry method resistant to shoulder-surfing and recording attacks* (Doctoral dissertation, University of Malaya). ProQuest Dissertations Publishing. https://www.proquest.com/openview/7cb62a0492aa907c0b636dc19e08fdc6/1?pq-origsite=gscholar&cbl=2026366&diss=y

Chaithra, I. V., Gowda, K. B. L., Pragna, L. S., Minal, J. J., Sinchana, S. D., & Prasad, M. J. (2025, April 28–29). Enhancing data security using Rubik's encryption and CNN model for biometric authentication. In *Proceedings of the 3rd IEEE International Conference on Knowledge Engineering and Communication Systems (ICKECS 2025)* (pp. 1–8). IEEE. https://doi.org/10.1109/ICKECS65700.2025.11035364

Chatterjee, S. R. (2019). [Exact dissertation title] (Doctoral dissertation, Cornell University). Cornell University eCommons. bank

Cheah, J.-H., Thurasamy, R., Memon, M. A., Chuah, F., & Ting, H. (2020). Multigroup analysis using SmartPLS: Step-by-step guidelines for business research. *Asian Journal of Business Research*, *10*(3). https://doi.org/10.14707/ajbr.200087

Cheng, E. W. (2018). Choosing between the theory of planned behavior (TPB) and the technology acceptance model (TAM). *Educational Technology Research and Development, 67*(1), 21–37. https://doi.org/10.1007/s11423-018-9598-6

Chin, W. W. (1998). The partial least squares approach for structural equation modeling. In G. A. Marcoulides (Eds.), Modern methods for business research (pp. 295 236). London: Lawrence Erlbaum Associates.

Chin WW. The partial least squares approach to structural equation modeling. Modern Methods for Business Research/ Lawrence Erlbaum Associates. 1998.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences*. https://doi.org/10.4324/9780203771587

Daoud, J. I. (2017). Multicollinearity and regression analysis. *Journal of Physics: Conference Series*, *949*, 012009. https://doi.org/10.1088/1742-6596/949/1/012009

Das, K. R., & Imon, A. H. M. R. (2016). A brief review of tests for normality. *American Journal of Theoretical and Applied Statistics, 5*(1), 5–12. https://doi.org/10.11648/j.ajtas.20160501.12

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319. https://doi.org/10.2307/249008

Davis, F. D. (1993). User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies, 38*(3), 475–487.

Dhagarra, D., Goswami, M., & Kumar, G. (2020). Impact of trust and privacy concerns on technology acceptance in healthcare: An Indian perspective. *International Journal of Medical Informatics, 141*, 104164. https://doi.org/10.1016/j.ijmedinf.2020.104164

Doddipatla, L., Ramadugu, R., Yerram, R. R., & Sharma, S. T. (2021). Exploring the role of biometric authentication in modern payment solutions. *International Journal of Digital Innovation, 2*(1). Research Workx. https://researchworkx.com/index.php/ijdi

Domingo, Ma. A., Bernadas, A. G., Maiquez, J. D., Ong, A. K., & Magana, M. C. (2025). Assessing the acceptance of palm biometric payment systems: An integration of technology acceptance model and valence framework. *Acta Psychologica, 259*, 105426. https://doi.org/10.1016/j.actpsy.2025.105426

Dong, Z., He, C., Hu, T., & Jiang, T. (2024). Integrating values, ascribed responsibility and environmental concern to predict customers' intention to visit green hotels: The mediating role of personal norm. *Frontiers in Psychology, 14*, 1340491. https://doi.org/10.3389/fpsyg.2023.1340491

Elmir, N. (2018). *An examination of biometric authentication adoption in the Canadian banking industry* (Doctoral dissertation, Athabasca University). ProQuest Dissertations Publishing. https://www.proquest.com/openview/f44aa48ac3a1bb644c5328441c2c380e/1?pq-origsite=gscholar&cbl=18750&diss=y

Erwin, H. A., Rithmaya, C. L., & Sekarsari, L. A. (2025). Biometric technology in digital banking: Insights from generation Z and millennials. *Journal of*

Business & Banking, *15*(01), 39–58. https://doi.org/10.14414/jbb.v15i1.5378

Etikan, I. (2016). Comparison of convenience sampling and purposive sampling. American Journal of Theoretical and https://doi.org/10.11648/j.ajtas.20160501.11

Faqih, K. M., & Jaradat, M.-I. R. (2015). Mobile healthcare adoption among patients in a developing country environment: Exploring the influence of age and gender differences. *International Business Research*, *8*(9). https://doi.org/10.5539/ibr.v8n9p142

Fulk, G. (2023). Descriptive statistics: An important first step. *Journal of Neurologic Physical Therapy*, *47*(2), 63–65. https://doi.org/10.1097/NPT.0000000000000434

Gao, W., Jiang, N., & Guo, Q. (2025). Facial recognition payment is cool: Coolness, inspiration, and customer continuance intention to use facial recognition payment. *Financial Innovation*, *11*(1). https://doi.org/10.1186/s40854-024-00697-1

Hamad, A. A., & Ahmed, S. K. (2025). Understanding the lower and upper limits of sample sizes in clinical research. *Cureus*. https://doi.org/10.7759/cureus.76724

Han, J., & Ko, D. (2025). Mobile financial service adoption among elderly consumers: The roles of technology anxiety, familiarity, and age. *FinTech*, *4*(3), 36. https://doi.org/10.3390/fintech4030036

Hair, J. F., Hult, G. T., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). Partial least squares structural equation modeling (PLS-SEM) using R. *Classroom Companion: Business*. https://doi.org/10.1007/978-3-030-80519-7

Harris, J. (2024, July 9). Billions hit by largest worldwide password leak - check yours now or risk theft. *The US Sun*. https://www.the-sun.com/tech/11871398/largest-ever-password-database-10-billion-leaked-warning/

Hung, M. C., & Jen, W. Y. (2012). The adoption of mobile health management services: An empirical study. *Journal of Medical Systems, 36*(3), 1381–1388. http://dx.doi.org/10.1007/s10916-010-9600-2

Hustava Sipulova, M., Taborecka, J., & Valova, H. (2025). Exploring perceptions and utilization of biometric technologies from consumer perspective. *International Review of Management and Marketing, 15*(3), 391–397. https://doi.org/10.32479/irmm.18817

Idika, D. O., Owan, V. J., & Agama, V. U. (2023). The application of the nominal scale of measurement in research data analysis. *Prestige Journal of Education, 6*(1), 190–198. Association for the Promotion of Innovation in Education (APIE). https://www.researchgate.net/publication/372157077

Islam, M. (2020). Data Analysis: Types, Process, Methods, Techniques and Tools. International Journal on Data Science and Technology. Vol. 6, No. 1, pp. 10-15. doi: 10.11648/j.ijdst.20200601.12

Joshi, A., Kale, S., Chandel, S., & Pal, D. K. (2015). Likert scale: Explored and explained. *British Journal of Applied Science & Technology, 7*(4), 396–403. https://doi.org/10.9734/BJAST/2015/14975

Kanak, A., & Sogukpinar, I. (2017). BIOTAM: A technology acceptance model for biometric authentication systems. *IET Biometrics, 6*(6), 457–467. https://doi.org/10.1049/iet-bmt.2016.0148

Khayer, A. (2024). Biometrics authentication for E-payment. *Jahangirnagar University Journal of Business Research, 23*(2), 147–166. https://doi.org/10.53461/jujbr.v23i2.27

Khade, S., Ahirrao, S., Phansalkar, S., Kotecha, K., Gite, S., & Thepade, S. D. (2021). Iris liveness detection for biometric authentication: A systematic literature review and future directions. *Inventions, 6*(4), 65. https://doi.org/10.3390/inventions6040065

Kitsiou, A., Despotidi, C., Kalloniatis, C., & Gritzalis, S. (2022). The role of users' demographic and social attributes for accepting biometric systems: A Greek case study. *Future Internet, 14*(11), 328. https://doi.org/10.3390/fi14110328

Kim, H.-Y. (2013). Statistical notes for clinical researchers: Assessing normal distribution (2) using skewness and kurtosis. *Restorative Dentistry & Endodontics, 38*(1), 52–54. https://doi.org/10.5395/rde.2013.38.1.52

Kim, J. H. (2019). Multicollinearity and misleading statistical results. *Korean Journal of Anesthesiology, 72*(6), 558–569. https://doi.org/10.4097/kja.19087

Kim, S. H., & Yoo, B. K. (2020). Factors influencing the reuse of mobile payment services in retail. 유통과학연구, 18(3), 53-65.

Kruzikova, A., Knapova, L., Smahel, D., Dedkova, L., & Matyas, V. (2022). Usable and secure? User perception of four authentication methods for mobile banking. *Computers & Security*, *115*, 102603. https://doi.org/10.1016/j.cose.2022.102603

Kumalasari, R. A., Rahardjo, K., Kusumawati, A., & Sunarti, S. (2024). Biometric-based self-service technology adoption by older adult: Empirical evidence from pension fund sector in Indonesia. *Cogent Business & Management*, *11*(1). https://doi.org/10.1080/23311975.2024.2325543

Kusairi, K., Sukmawati, A., A.S, N., & Rahman, M. S. (2025). Predicting M-banking adoption: The moderating role of age in technology acceptance. *Cogent Business & Management*, *12*(1). https://doi.org/10.1080/23311975.2025.2547964

Lancelot Miltgen, C., Popovič, A., & Oliveira, T. (2013). Determinants of end-user acceptance of biometrics: Integrating the "big 3" of technology acceptance with privacy context. *Decision Support Systems*, *56*, 103–114. https://doi.org/10.1016/j.dss.2013.05.010

Leon, A. C., Davis, L. L., & Kraemer, H. C. (2011). The role and interpretation of pilot studies in clinical research. *Journal of Psychiatric Research*, *45*(5), 626–629. https://doi.org/10.1016/j.jpsychires.2010.10.008

Lien, C.-W., & Vhaduri, S. (2023). Challenges and opportunities of biometric user authentication in the age of IOT: A survey. *ACM Computing Surveys*, *56*(1), 1–37. https://doi.org/10.1145/3603705

Liu, M., Wang, C., & Hu, J. (2025). Understanding older adults' adoption of facial recognition payment: An integrated model of Tam and UXT. *PLOS One*, *20*(7). https://doi.org/10.1371/journal.pone.0325291

Loeb, S., Dynarski, S., McFarland, D., Morris, P., Reardon, S., & Reber, S. (2017, March). NCEE publications: Descriptive Analysis in Education: A Guide for Researchers. Institute of Education Sciences (IES) Home Page, a part of the

U.S. Department of Education. Retrieved March 21, 2023, from https://ies.ed.gov/ncee/pubs/20174023/

Lovisotto, G., Malik, R., Sluganovic, I., Roeschlin, M., Trueman, P., & Martinovic, I. (2017). *Mobile biometrics in financial services: A five-factor framework* (CS-RR-17-03). Department of Computer Science, University of Oxford. https://api.semanticscholar.org/CorpusID:36245238

Maixé-Altés, J. C. (2021). Reliability and security at the dawn of Electronic Bank transfers in the 1970s-1980s. *Revista de Historia Industrial. Economía y Empresa*, *30*(81), 151–187. https://doi.org/10.1344/rhi.v30i81.31405

M. A. Noori and Madam Norleyza Jailani, "Biometric authentication technology acceptance in mobile banking in Iraq," Jul. 2022. doi: 10.14704/nq.2022.20.7. NQ33378.

Markert, P., Bailey, D. V., Golla, M., Dürmuth, M., & Aviv, A. J. (2021). On the security of smartphone unlock pins. *ACM Transactions on Privacy and Security*, *24*(4), 1–36. https://doi.org/10.1145/3473040

Mat Nawi, F. A., Mamat, M., Baistaman, J., Setapa, M., & Ramli, N. H. (2022). The SEM smartpls model assessment: Mediating influence of Technology Infrastructure support on Human Capital Determinants in TVET institutions. *International Journal of Academic Research in Business and Social Sciences*, *12*(11). https://doi.org/10.6007/ijarbss/v12-i11/15410

Memon, M. A., Ting, H., Cheah, J.-H., Thurasamy, R., Chuah, F., & Cham, T. H. (2020). Sample Size For Survey Research: Review and recommendations. Journal of Applied Structural Equation Modeling, 4(2), i-xx. https://doi.org/10.47263/jasem.4(2)01

Md Kassim, N. (2024). Impact on effectiveness usage of biometrics towards internet banking continuance usage among Malaysians. *Global Business and Management Research: An International Journal, 16*(4s), 1979–1996.

Miskan, N. H., Hussin, N. L., Muhamad, N., Mohd Esa, M., & Mohd Aziz, N. E. (2021b). The financial technology (M-banking) adoption among baby-boomers in twenty-First Century. *International Journal of Academic Research in Business and Social Sciences*, *11*(8). https://doi.org/10.6007/ijarbss/v11-i8/10703

Mohd, S. N. H., Hashim, H., Shafee, N., Suhaimi, S., & Tan, Y. Z. (2025). Extending the valence framework: Factors influencing Malaysians' intention to adopt facial recognition payment systems. *Journal of Logistics, Informatics and Service Science*. https://doi.org/10.33168/jliss.2025.0308

Moradi, M., Moradkhani, M., & Tavakoli, M. B. (2022). Security-level improvement of iot-based systems using biometric features. *Wireless Communications and Mobile Computing, 2022*(1). https://doi.org/10.1155/2022/8051905

M. Rukhiran, S. Wong-In, and P. Netinant, "User Acceptance Factors Related to Biometric Recognition Technologies of Examination Attendance in Higher Education: TAM Model," Sustainability, vol. 15, no. 4, p. 3092, Feb. 2023, doi: 10.3390/su15043092.

MyCERT: Home. (2024). https://www.mycert.org.my/

Naeem, S. (2019, June 6). Data editing in research. Helping Research writing for student & professional researchers. Retrieved March 19, https://researcharticles.com/index.php/data-editing-in-research/ 2023, from

Nan, D., Kim, Y., Huang, J., Jung, H. S., & Kim, J. H. (2022). Factors affecting intention of consumers in using face recognition payment in offline markets: An acceptance model for future payment service. *Frontiers in Psychology*, *13*. https://doi.org/10.3389/fpsyg.2022.830152

Nanda, A., Jeong, J. J., Shah, S. W., Nosouhi, M., & Doss, R. (2024). Examining usable security features and user perceptions of physical authentication devices. *Computers & Security*, *139*, 103664. https://doi.org/10.1016/j.cose.2023.103664

Natarajan, T., Balasubramanian, S. A., & Kasilingam, D. L. (2018). The moderating role of device type and age of users on the intention to use mobile shopping applications. *Technology in Society*, *53*, 79–90. https://doi.org/10.1016/j.techsoc.2018.01.003

Onwuegbuzie, A., & Leech, N. (2015). Sampling designs in qualitative research: Making the sampling process more public. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2007.1636

Pereira, L. M., Sanchez Rodrigues, V, & Freires, F. G. (2024). Use of partial least squares structural equation modeling (PLS-SEM) to improve plastic waste

management. *Applied Sciences*, *14*(2), 628. https://doi.org/10.3390/app14020628

Peres, R., Muller, E., & Mahajan, V. (2010). Innovation diffusion and new product growth models: A critical review and research directions. International journal of research in marketing, 27(2), 91-106

Phuoc, Nguyen Van. 2022. The Critical Factors Impacting Artificial Intelligence Applications Adoption in Vietnam: A Structural Equation Modeling Analysis. Economies 10: 129. https://doi.org/ 10.3390/economies10060129

Piotrowska, A. I. (2024). Determinants of consumer adoption of biometric technologies in Mobile Financial Applications. *Economics and Business Review*, *10*(1). https://doi.org/10.18559/ebr.2024.1.1019

Poulsen, R., Tan, D. W., Sowman, P. F., McAlpine, D., & Pellicano, E. (2025). Auditory environments influence the link between Autistic traits and quality of life. *Scientific Reports, 15*, 10612. https://doi.org/10.1038/s41598-025-94585-y

Rawat, A. S. (2021, March 31). What is descriptive analysis?- types and advantages: Analytics steps. What is Descriptive Analysis?- Types and Advantages | Analytics Steps. Retrieved March 20, 2023, from https://www.analyticssteps.com/blogs/overview-descriptive analysis

Ruhani, A. B., Mansor, N. S., Awang, H., Zolkipli, M. F., Zaini, K. M., & Benlahcene, A. (2024). Modelling security factors influencing E-wallet adoption in Malaysia. *Iraqi Journal for Computer Science and Mathematics*, *5*(4). https://doi.org/10.52866/2788-7421.1205

Rukhiran, M., Wong-In, S., & Netinant, P. (2023). User acceptance factors related to biometric recognition technologies of examination attendance in Higher Education: TAM model. *Sustainability*, *15*(4), 3092. https://doi.org/10.3390/su15043092

Safuri, N. H., Ram Sing, R. D., & Sing, K. K. (2024). Key drivers of gen Z's digital banking adoption in Malaysia: The roles of Relative Advantage, trust, and perceived value as a mediator. *International Journal of Academic Research in Business and Social Sciences, 14*(12). https://doi.org/10.6007/ijarbss/v14-i12/24237

Saunders, M. N. K., Lewis, P., &Thornhill, A. (2016). *Research methods for business students* (Seventh edition). Pearson Education.

Sharma, B. (2016). A focus on reliability in developmental research through Cronbach's alpha among medical, dental and paramedical professionals. *Asian Pacific Journal of Health Sciences*, *3*(4), 271–278. https://doi.org/10.21276/apjhs.2016.3.4.43

Sekaran, U., & Bougie, R. (2010). Research methods for business: A skill building approach (5th ed.). West Sussex, UK: John Wiley & Sons Ltd.

Showkat, N., & Parveen, H. (2017, July). Non-Probability and Probability Sampling. Retrieved March 9, https://www.researchgate.net/publication/319066480_Non Probability_and_Probability_Sampling

Smith, S. A. (2002). *An evaluation of response scale formats of the culture assessment instrument* (Doctoral dissertation, Rand Afrikaans University).

Stevens, S. S. (1946). On the theory of scales of measurement. *Science, 103*(2684), 677–680. https://doi.org/10.1126/science.103.2684.677

Stylios, I., Kokolakis, S., Thanou, O., & Chatzis, S. (2021). Behavioral Biometrics & continuous user authentication on mobile devices: A survey. *Information Fusion, 66*, 76–99. https://doi.org/10.1016/j.inffus.2020.08.021

Sultana, N., & Akter, T. (2025). IOT biometric technology adoption in higher education: A tram-based analysis of users and non-users in Bangladesh. *Discover Internet of Things*, *5*(1). https://doi.org/10.1007/s43926-025-00204-7

Taherdoost, H. (2021). Data Collection Methods and Tools for Research; A Step-by-Step Guide to Choose Data Collection Technique for Academic and Business Research Projects. International Journal of Academic Research in Management (IJARM), 2021, 10 (1), pp.10-38. hal-03741847

Thodenius, B., Bátiz-Lazo, B., & Karlsson, T. (2011). The history of the Swedish ATM: Sparfrämjandet and metior. *IFIP Advances in Information and Communication Technology*, 92–100. https://doi.org/10.1007/978-3-642-23315-9_11

Venkatesh, Morris, Davis, & Davis. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425. https://doi.org/10.2307/30036540

Wahid, L. O., & Pratama, A. R. (2022). Factors influencing smartphone owners' acceptance of biometric authentication methods. *ILKOM Jurnal Ilmiah*, *14*(2), 91–98. https://doi.org/10.33096/ilkom.v14i2.1114.91-98

Wang, J. S. (2021). Exploring biometric identification in fintech applications based on the modified Tam. *Financial Innovation*, *7*(1). https://doi.org/10.1186/s40854-021-00260-2

Wan Nawang, W. R., & Syabil Nazhan Ahd.Moess. (2023). Predicting intention to use QR code mobile payment among Malaysian Muslim millennials. *The Journal of Muamalat and Islamic Finance Research*, 49–63. https://doi.org/10.33102/jmifr.481

Wong, K. K.-K. (2013, January). (PDF) Partial Least Square Structural Equation Modeling (PLS-SEM) techniques using smartpls. https://www.researchgate.net/publication/268449353_Partial_least_square_structural_equation_modeling_PLS-SEM_techniques_using_SmartPLS

Xue, Y., Bradley, J., & Liang, H. (2011). Team climate, empowering leadership, and knowledge sharing. *Journal of Knowledge Management*, *15*(2), 299–312. https://doi.org/10.1108/13673271111119709

Yağar, F. (2021). Fear of COVID-19 and its association with health literacy in elderly patients. *Journal of Patient Experience*, *8*, 1–6. https://doi.org/10.1177/23743735211056506

Zhang, J. (2024). Influential factors impacting users' behavioral intentions regarding facial recognition payment systems of mobile payment platforms in Wuhan, China. *AU-GSB e-Journal*, *17*(3), 59–70. Assumption University of Thailand. http://www.assumptionjournal.au.edu/index.php/AU-GSB/index

Zhang, J., Liu, Z., & Luo, X. (Robert). (2024). Unraveling juxtaposed effects of biometric characteristics on user security behaviors: A controversial information technology perspective. *Decision Support Systems*, *183*, 114267. https://doi.org/10.1016/j.dss.2024.114267

Zhang, Y. (2024). Impact of perceived privacy and security in the TAM model: The Perceived Trust as the mediated factors. *International Journal of Information Management Data Insights*, *4*(2), 100270. https://doi.org/10.1016/j.jjimei.2024.100270

Zihan Kalila Gusnan, & Rio Guntur Utomo. (2024). Factors affecting user's acceptance of adopting biometrics technologies using the TAM model. *Jurnal Teknik Informatika (Jutif)*, *5*(4), 309–320. https://doi.org/10.52436/1.jutif.2024.5.4.2249

Zimmermann, V. (2021). *[Exact title of dissertation]* (Doctoral dissertation, Technische Universität Darmstadt). TUprints. https://doi.org/10.26083/tuprints-00017425

Zikmund, W. G., Babin, B. J., Carr, J. C., & Griffin, M. (2013). *Business research methods* (9th ed.). Cengage Learning.

APPENDICES

Appendix 3.1: Questionnaire

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF ACCOUNTANCY AND MANAGEMENT

BACHELOR OF Finance (Financial Technology)

(HONS)

Factor Influencing Consumer Intention to Adopt Biometric Authentication

Survey Questionnaire

Dear Valued Respondents,

I am conducting an academic research study as part of my Final Year Project at Universiti Tunku Abdul Rahman (UTAR), Sungai Long Campus, currently studying Bachelor of Finance (Financial Technology) with Honours.

This research project investigates the factors influencing consumer intention to adopt biometric authentication. The questionnaire consists of two (2) sections and will take approximately 10-15 minutes to complete. Kindly answer all questions in both sections. Your participation is entirely voluntary, and all information provided will be kept strictly confidential

Your valuable input will contribute significantly to the advancement of knowledge in this field. Thank you for your participation and support.

Warm regards,

Ivy Lu Zi Ying

Email: luziying1@1utar.my

Email: _____

PERSONAL DATA PROTECTION NOTICE

Please be informed that in accordance with Personal Data Protection Act 2010 ("PDPA") which came into force on 15 November 2013, Universiti Tunku Abdul Rahman ("UTAR") is hereby bound to make notice and require consent in relation to collection, recording, storage, usage and retention of personal information.

1. Personal data refers to any information which may directly or indirectly identify a person which could include sensitive personal data and expression of opinion. Among others it includes:

a) Name
b) Identity card
c) Place of Birth
d) Address
e) Education History
f) Employment History
g) Medical History
h) Blood type
i) Race
j) Religion
k) Photo

l) Personal Information and Associated Research Data

2. The purposes for which your personal data may be used are inclusive but not limited to:

a) For assessment of any application to UTAR
b) For processing any benefits and services
c) For communication purposes
d) For advertorial and news
e) For general administration and record purposes
f) For enhancing the value of education
g) For educational and related purposes consequential to UTAR
h) For replying any responds to complaints and enquiries
i) For the purpose of our corporate governance
j) For the purposes of conducting research/ collaboration

3.Your personal data may be transferred and/or disclosed to third party and/or UTAR collaborative partners including but not limited to the respective and appointed outsourcing agents for purpose of fulfilling our obligations to you in respect of the purposes and all such other purposes that are related to the purposes

and also in providing integrated services, maintaining and storing records. Your data may be shared when required by laws and when disclosure is necessary to comply with applicable laws.

4. Any personal information retained by UTAR shall be destroyed and/or deleted in accordance with our retention policy applicable for us in the event such information is no longer required.

5. UTAR is committed in ensuring the confidentiality, protection, security and accuracy of your personal information made available to us and it has been our ongoing strict policy to ensure that your personal information is accurate, complete, not misleading and updated. UTAR would also ensure that your personal data shall not be used for political and commercial purposes.

Consent:

6. By submitting or providing your personal data to UTAR, you had consented and agreed for your personal data to be used in accordance to the terms and conditions in the Notice and our relevant policy.

7. If you do not consent or subsequently withdraw your consent to the processing and disclosure of your personal data, UTAR will not be able to fulfill our obligations or to contact you or to assist you in respect of the purposes and/or for any other purposes related to the purpose.

Acknowledgment of Notice

- □ I have been notified and that I hereby understood, consented and agreed per UTAR above notice.
- □ I disagree, my personal data will not be processed.

Usage of biometrics authentication

⚠ Please answer carefully. If you select No by mistake, the survey will end automatically and you will not proceed to the next sections.

Have you ever used biometric authentication (e.g., fingerprint, face recognition, voice recognition) for login or transactions?

- □ Yes
- □ No

Section A: Demographic Question

1. Please select your gender.
   - □ Male
   - □ Female

2. Please select your age group.

- 28 or less
- 29 – 44
- 45 – 60
- 61 – 79
- 80 and above

3. Please select your education levels. If it is not listed in the options, choose "Others" and specify.
   - Secondary / SPM / UEC
   - Foundation
   - Diploma
   - Bachelor's Degree
   - Master's Degree and above
   - Other: _____

Section B: Variable Question

This section seeks your opinions on the factors that may influence your intention to adopt biometric authentication (e.g., fingerprint, facial recognition, voice recognition) in digital financial services and online applications. Respondents are asked to indicate the extent to which they agree or disagree with each statement using a 5-point Likert scale:

Note: 1= Strongly Disagree (SD), 2= Disagree (D), 3= Neutral (N), 4= Agree (A), 5= Strongly Agree (SA)

Please select one response per statement to indicate the extent to which you agree or disagree with the following items.

Question / Items		**Evaluation Scale**				
Perceived Usefulness (PU)		**SD**	**D**	**N**	**A**	**SA**
1	Using biometric authentication enhances the productivity of my digital financial activities.	1	2	3	4	5
2	Using biometric authentication enables me to accomplish tasks more quickly					
3	Using biometric authentication provides valuable benefits for me.					
4	Using biometric authentication makes it easier for me to carry out activities.					
5	I find biometric authentication useful in performing my activities such as secure financial and digital activities.					

Question / Items		Evaluation Scale				
Perceived Ease of Use (PEOU)		**SD**	**D**	**N**	**A**	**SA**
1	It is easy for me to use biometric authentication.	1	2	3	4	5
2	Learning to use biometric authentication would be easy for me.					
3	I find it easy to get biometric authentication to do what I want it to do.					
4	It is clear and easy for me to understand how to use biometric authentication.					
5	It is easy for me to accomplish what I need by using biometric authentication.					

Question / Items		Evaluation Scale				
Security and Privacy Risk (SPR)		**SD**	**D**	**N**	**A**	**SA**
1	It is likely that someone may get access to my accounts by bypassing biometric authentication.	1	2	3	4	5
2	It is likely that someone may break into my online accounts by bypassing biometric authentication.					
3	It is likely that someone may use biometric authentication on my device for unauthorized payments.					
4	I may get unauthorized charges on my accounts even when using biometric authentication.					
5	It is likely that someone may steal my device and gain access to my personal data even with biometric authentication.					

Question / Items		Evaluation Scale				
Behavioral intention to adopt biometric authentication (BI)		**SD**	**D**	**N**	**A**	**SA**
1	I intend to adopt Biometric Authentication technology as soon as possible.	1	2	3	4	5
2	I prefer biometric authentication over traditional methods (e.g.Passwords/PINs).					
3	I will use biometric authentication whenever it is available (e.g., when I need to verify my identity).					
4	I intend to use the mobile phone to perform Biometric Authentication behaviours frequently.					
5	It is likely that I will use my mobile phone to perform biometric authentication in the future.					

Actual use behaviour to adopt biometric authentication

Question / Items		**Evaluation Scale**				
Actual use behaviour to adopt biometric authentication		**SD**	**D**	**N**	**A**	**SA**
1	I have used biometric authentication when it is available.	1	2	3	4	5
2	I have used biometric authentication many times during a typical week.					
3	I am very likely to continue using biometric authentication in the future.					
4	I think using biometric authentication is worth it.					
5	I would recommend using biometric authentication to others.					

Thank You for your participation

Thank you for completing this survey. Your participation is greatly appreciated and will contribute to the success of this research. Your valuable input will be of great help to me in completing my study, and I am truly grateful for your time and effort.

If you have any question regarding this questionnaire, please feel free to contact me at luziying1@1utar.my

Appendix 3.4.2: Pilot Test Result

Perceived Usefulness (PU)

Reliability Statistics

Cronbach's Alpha	N of Items
.888	5

Perceived Ease of Use (PEOU)

Reliability Statistics

Cronbach's Alpha	N of Items
.921	5

Security and Privacy Risks (SPR)

Reliability Statistics

Cronbach's Alpha	N of Items
.924	5

Behaviour Intention (BI)

Reliability Statistics

Cronbach's Alpha	N of Items
.891	5

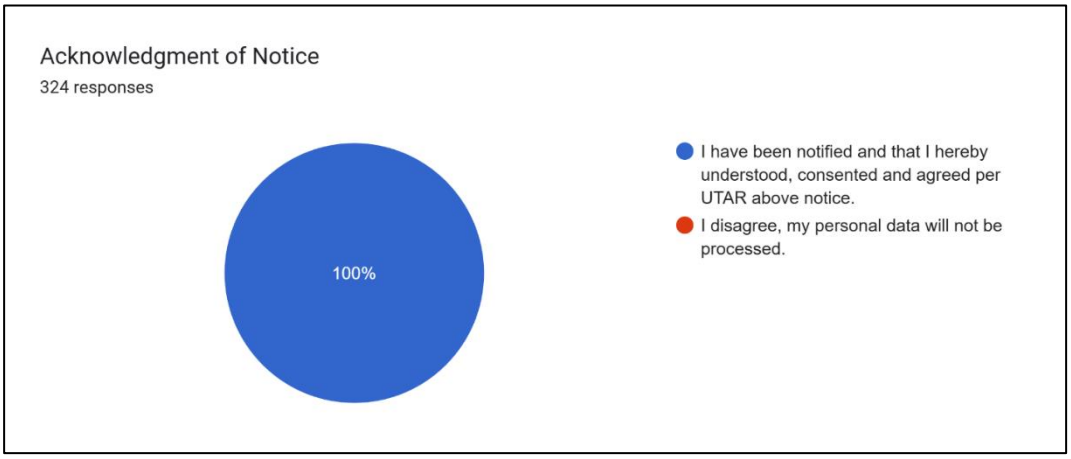
Actual Usage Behaviour (AU)

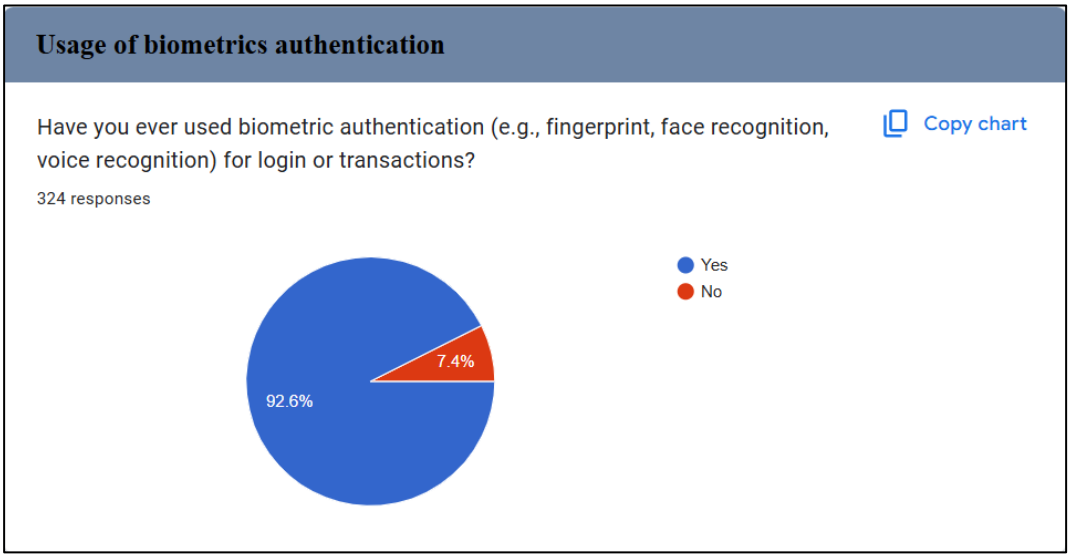
Reliability Statistics

Cronbach's Alpha	N of Items
.927	5

Appendix 4.1: Survey Respondent

Result of Personal Data Protection notice

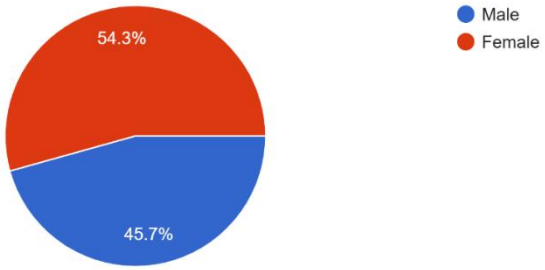




Section A： Demographics result – of respondent

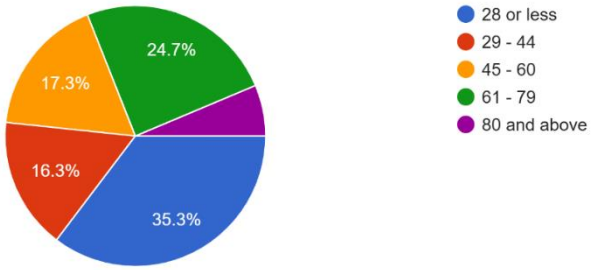
1. Please select your gender.

300 responses



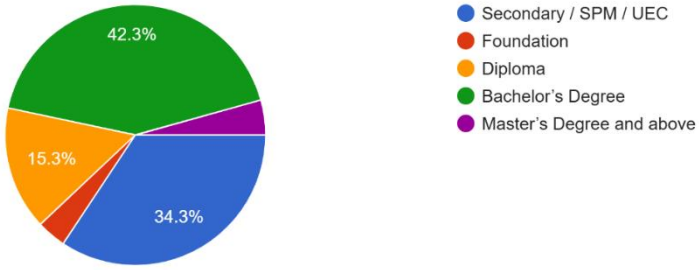
2. Please select your age group.

300 responses

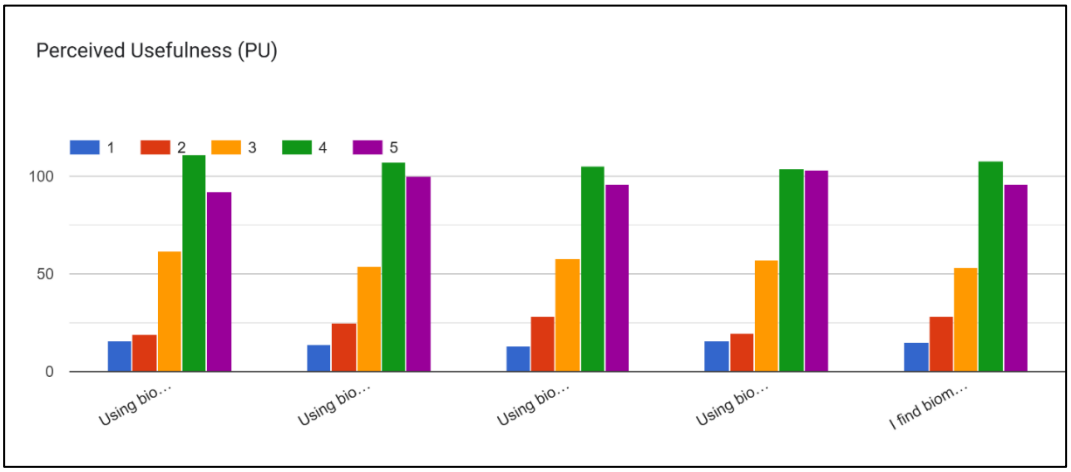


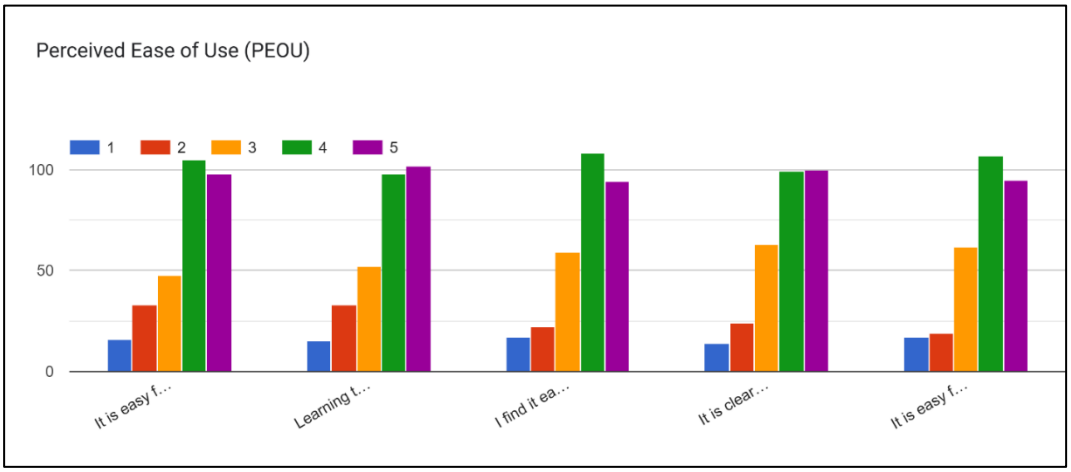
3. Please select your education levels. If it is not listed in the options, choose "Others" and specify.

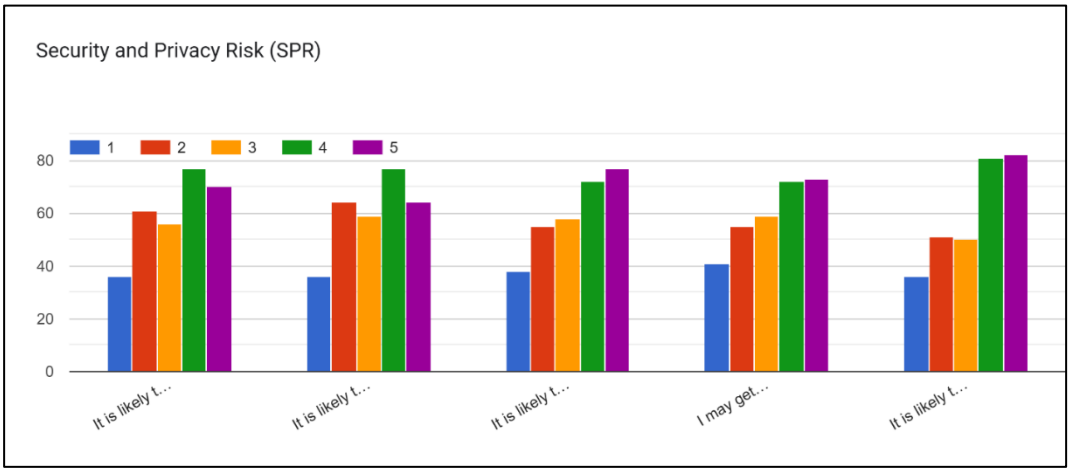
300 responses

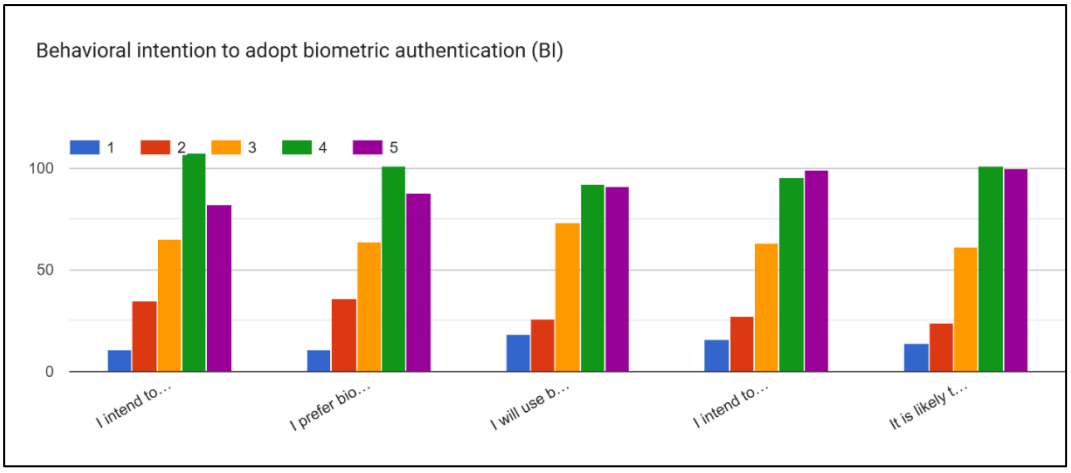


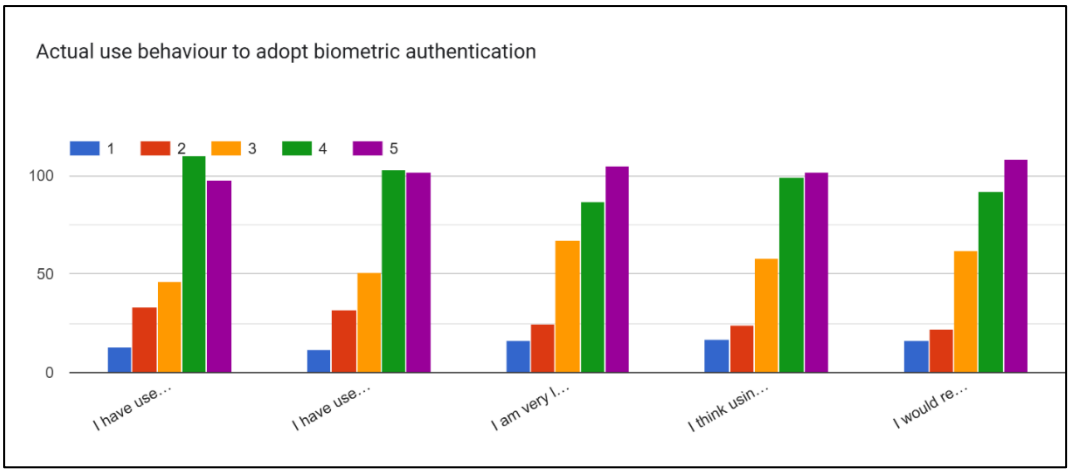
Section B： Variable Question result – of respondent








Behavioral intention to adopt biometric authentication (BI)
1
2
3
4
5
100
50
0
I intend to...
I prefer bio...
I will use b...
I intend to...
It is likely t...


Actual use behaviour to adopt biometric authentication
1
2
3
4
5
100
50
0
I have use...
I have use...
I am very l...
I think usin...
I would re...