UNIVERSITI
MALAYSIA
KELANTAN

**FACULTY OF ENTREPRENEURSHIP AND BUSINESS**

**FINAL YEAR RESEARCH PROJECT**

# IMPACT OF SECURITY FACTORS TOWARDS E-BANKING USAGE INTENTION IN MALAYSIA

| | |
|---|---|
| **Programme** | Sarjana Muda Pentadbiran Perniagaan<br>(Perbankan Dan Kewangan Islam) Dengan Kepujian (SAB) |
| **Name of Supervisor** | Dr Azira Hanani Binti Ab Rahman |
| **Name of Examiner** | Dr Siti Nurzahira Binti Che Tahrim |
| **Name of Students** | i. Nurul Nabilah Binti Azme (A18B0734)<br>ii. Ruli Akhbar Bin Hendi (A18A1137)<br>iii. Siti Maisarah Binti Ahmadi (A18A1143)<br>iv. Siti Nur-Nadzirah Amanina Binti Abdullah (A18A1147) |
| **Date** | 20th January 2022 |

UMK/AKAD/P&P/FK05

# REKOD PENERIMAAN TUGASAN PELAJAR
## *RECORD OF RECEIPT OF STUDENT'S ASSIGNMENT*

Kod/ Nama Kursus: AFS4112/ Projek Penyelidikan Perbankan dan Kewangan Islam I
*Code/ Course Name: AFS4112/*

Sesi/ *Session:* 2020/2021
Semester*:* Februari

Nama Program/ *Name of Programme:* SAB
Fakulti/ Pusat/ *Faculty/ Centre:* Fakulti Keusahawanan dan Perniagaan

| ***No.*** | **Tarikh**<br>***Date*** | **Nama Pelajar**<br>***Student's Name*** | **No. Matriks**<br>***Matrix No.*** | **Tandatangan**<br>***Signature*** | | **Catatan**<br>***Remarks*** |
|---|---|---|---|---|---|---|
| | | | | **Pelajar**<br>***Student*** | **Pensyarah**<br>***Lecturer*** | |
| 1 | 16/6/2021 | Ruli Akhbar Bin Hendi | A18A1137 | | | |
| 2 | 16/6/2021 | Nurul Nabilah Binti Azme | A18B0734 | | | |
| 3 | 16/6/2021 | Siti Nur-Nadzirah Amanina Binti Abdullah | A18A1147 | | | |
| 4 | 16/6/2021 | Siti Maisarah Binti Ahmadi | A18A1143 | | | |

**UMK/FKP/PPTA/01**

UNIVERSITI
MALAYSIA
KELANTAN

**FAKULTI KEUSAHAWANAN DAN PERNIAGAAN**
**UNIVERSITI MALAYSIA KELANTAN**

**BORANG KELULUSAN PENYERAHAN**
**LAPORAN AKHIR PROJEK PENYELIDIKAN TANPA JILID**

Kepada,

Dekan,
Fakulti Keusahawanan dan Perniagaan
Universiti Malaysia Kelantan

**Kelulusan Penyerahan Draf Akhir Laporan Akhir Projek Penyelidikan Tahun Akhir Tanpa Jilid**

Saya, ........................................................................................., penyelia kepada pelajar berikut, bersetuju membenarkan penyerahan dua (2) naskah draf akhir Laporan Akhir Projek Penyelidikan Tahun Akhir tanpa jilid untuk pentaksiran.

**Nama Pelajar:** ______________________________ **No Matrik:** ________________

**Tajuk Penyelidikan:**

______________________________________________________________________

______________________________________________________________________

Sekian, terima kasih

____________________
Tandatangan Penyelia

Tarikh:

**UMK/FKP/PPTA/03**

Universiti Malaysia
KELANTAN

## REKOD PENGESAHAN PENYARINGAN *TURNITIN*
## *VERIFICATION RECORD OF TURNITIN SCREENING*

Kod/Nama Kursus*:*
*Code/ Course Name:*
Sesi/*Session:*
Semester*:*
Nama Program/*Name of Programme:* SAK, SAB, SAL, SAR, SAP, SAH, SAW
Fakulti/Pusat/*Faculty/Centre:* Fakulti Keusahawanan Dan Perniagaan/
*Faculty of Entrepreneurship and Business*

**Pengesahan Penyaringan Plagiat/ *Verification of Plagiarism Screening***

Saya,………………………………………………………………………………(Nama),No.Matrik ……………………………..……..dengan ini mengesahkan Kertas Projek Penyelidikan ini telah melalui saringan aplikasi turnitin. Bersama ini dilampirkan sesalinan laporan saringan Turnitin dengan skor persamaan sebanyak ………%.

*I,………………………………………………………………………………………………(Name), Matrix number ……………………………..……..hereby declare that I have screen my thesis using Turnitin Software. Enclosed here with a copy of verification of Turnitin screening with similarity score of ………%.*

Tajuk Kertas Kerja Penyelidikan/ *The Tittle of Research Project Paper*:-

………………………………………………………………………………………………………………

………………………………………………………………………………………………………………

Tandatangan/*Signature*

……..............................................

Nama Pelajar/*Student Name*:

No.Matrik/*Matrix No*:

Tarikh/*Date*:

Pengesahan
Penyelia/*Supervisor*:

Tandatangan/*Signature:*

Tarikh/*Date:*

**Research Topic: IMPACT OF SECURITY FACTORS TOWARDS E-BANKING USAGE INTENTION IN MALAYSIA**

## ASSESSMENT RUBRICS FOR RESEARCH PROJECT I: PRESENTATION (Weight 20%)

| NO. | CRITERIA | PERFORMANCE LEVEL | | | | Weight | TOTAL |
|---|---|---|---|---|---|---|---|
| | | POOR<br>(1 MARK) | FAIR<br>(2 MARKS) | GOOD<br>(3 MARKS) | EXCELLENT<br>(4 MARKS) | | |
| 1. | Teamwork<br>(CLO2; A3/TS) | Is not committed to work in a group | Is committed but make little effort to complete the research report in group | Is committed and make reasonable effort in completing the research report | Is very committed and make very good effort in completing the research report | ____ x 1<br>(Max: 4) | |
| 2. | Clear delivery of ideas<br>(CLO2; A3/CS) | Able to deliver ideas and require further improvement | Able to deliver ideas fairly clearly and require minor improvements | Able to deliver ideas clearly | Able to deliver ideas with great clarity | ____ x 1<br>(Max: 4) | |
| 3. | Effective and articulate delivery of ideas<br>(CLO2; A3/CS) | Able to deliver ideas with limited effect and require further improvement | Able to deliver ideas fairly effectively and require minor improvements | Able to deliver ideas effectively and articulately | Ability to deliver ideas with great effect and articulate | ____ x 1<br>(Max: 4) | |
| 4. | Appropriate use of visual aid<br>(CLO2; A3/CS) | Uses visual aids very poorly and the use interferes with the presentation | Uses visual aids but not very effective in aiding the presentation. The usage distorts the presentation at times | Uses visual aids effectively. The usage of technology flows with the presentation | Uses visual aids very effectively. The usage enhances the quality of presentation | ____ x 1<br>(Max: 4) | |
| 5. | Confidence and Ability to Answer Questions<br>(CLO2; A3/CT) | Exhibits a very low level of confidence and appears visibly 'shaky'. Finds it difficult to answer questions. | Exhibits low level of confidence at times. Does not appear to be confident in answering questions | Exhibits a high level confidence. Does a good job in answering questions. | Exhibits a very high level of confidence. Is perfectly at ease while answering questions. | ____ x 1<br>(Max: 4) | |
| | **TOTAL** | | | | | **/20** | |

## ASSESSMENT FORM FOR FINAL YEAR RESEARCH PROJECT: RESEARCH REPORT (Weight 50%)
## (COMPLETED BY SUPERVISOR AND EXAMINER)

**Student's Name:** ____________________________________________________________ **Matric No.** ______________________________

**Name of Supervisor:** ______________________________ **Name of Programme:** ________________________________________________

**Research Topic:** ____________________________________________________________________________________________________

| NO. | CRITERIA | PERFORMANCE LEVEL | | | | WEIGHT | TOTAL |
|---|---|---|---|---|---|---|---|
| | | **POOR (1 MARK)** | **FAIR (2 MARKS)** | **GOOD (3 MARKS)** | **EXCELLENT (4 MARKS)** | | |
| 1. | **Content (10 MARKS)**<br>(Research objective and Research Methodology in accordance to comprehensive literature review)<br>Content of report is systematic and scientific (Systematic includes Background of study, Problem Statement, Research Objective, Research Question) (Scientific refers to researchable topic) | Poorly clarified and not focused on Research objective and Research Methodology in accordance to comprehensive literature review. | Fairly defined and fairly focused on Research objective and Research Methodology in accordance to comprehensive literature review. | Good and clear of Research objective and Research Methodology in accordance to comprehensive literature review with good facts. | Strong and very clear of Research objective and Research Methodology in accordance to comprehensive literature review with very good facts. | ____ x 1.25<br>(Max: 5) | |
| | | Content of report is written unsystematic that not include Background of study, Problem Statement, Research Objective, Research Question and unscientific with unsearchable topic. | Content of report is written less systematic with include fairly Background of study, Problem Statement, Research Objective, Research Question and less scientific with fairly researchable topic. | Content of report is written systematic with include good Background of study, Problem Statement, Research Objective, Research Question and scientific with good researchable topic. | Content of report is written very systematic with excellent Background of study, Problem Statement, Research Objective, Research Question and scientific with very good researchable topic. | ____ x 1.25<br>(Max: 5) | |
| 2. | **Overall** ***Submit*** | The report is not | The report is produced | The report is | The report is | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **report format (5 MARKS)** | ***according to acquired format*** | produced according to the specified time and/ or according to the format | according to the specified time but fails to adhere to the format. | produced on time, adheres to the format but with few weaknesses. | produced on time, adheres to the format without any weaknesses. | ____ x 0.25<br>(Max: 1) | |
| | | ***Writing styles (clarity, expression of ideas and coherence)*** | The report is poorly written and difficult to read. Many points are not explained well. Flow of ideas is incoherent. | The report is adequately written; Some points lack clarity. Flow of ideas is less coherent. | The report is well written and easy to read; Majority of the points is well explained, and flow of ideas is coherent. | The report is written in an excellent manner and easy to read. All of the points made are crystal clear with coherent argument. | ____ x 0.25<br>(Max: 1) | |
| | | ***Technicality (Grammar, theory, logic and reasoning)*** | The report is grammatically, theoretically, technically and logically incorrect. | There are many errors in the report, grammatically, theoretically, technically and logically. | The report is grammatically, theoretically, technically and logically correct in most of the chapters with few weaknesses. | The report is grammatically, theoretically, technically, and logically perfect in all chapters without any weaknesses. | ____ x 0.25<br>(Max: 1) | |
| | | ***Reference list (APA Format)*** | No or incomplete reference list. | Incomplete reference list and/ or is not according to the format. | Complete reference list with few mistakes in format adherence. | Complete reference list according to format. | ____ x 0.25<br>(Max: 1) | |
| | | ***Format organizing (cover page, spacing, alignment, format structure, etc.)*** | Writing is disorganized and underdeveloped with no transitions or closure. | Writing is confused and loosely organized. Transitions are weak and closure is ineffective. | Uses correct writing format. Incorporates a coherent closure. | Writing include a strong beginning, middle, and end with clear transitions and a focused closure. | ____ x 0.25<br>(Max: 1) | |
| 3. | **Research Findings and Discussion (20 MARKS)** | | Data is not adequate and irrelevant. | Data is fairly adequate and irrelevant. | Data is adequate and relevant. | Data is adequate and very relevant. | ____ x 1<br>(Max: 4) | |
| | | | Measurement is wrong and irrelevant | Measurement is suitable and relevant but need major adjustment. | Measurement is suitable and relevant but need minor adjustment. | Measurement is excellent and very relevant. | ____ x 1<br>(Max: 4) | |

|  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|
|  |  | Data analysis is inaccurate | Data analysis is fairly done but needs major modification. | Data analysis is satisfactory but needs minor modification. | Data analysis is correct and accurate. | ____ x 1<br>(Max: 4) |  |
|  |  | Data analysis is not supported with relevant output/figures/tables and etc. | Data analysis is fairly supported with relevant output/figures/tables and etc. | Data analysis is adequately supported with relevant output/figures/table and etc. | Data analysis is strongly supported with relevant output/figures/table and etc. | ____ x 1<br>(Max: 4) |  |
|  |  | Interpretation on analyzed data is wrong. | Interpretation on analyzed data is weak. | Interpretation on analyzed data is satisfactory. | Interpretation on analyzed data is excellent | ____ x 1<br>(Max: 4) |  |
| 4. | **Conclusion and Recommendations (15 MARKS)** | Implication of study is not stated. | Implication of study is weak. | Implication of study is good. | Implication of study is excellent | ____ x 1.25<br>(Max: 5) |  |
|  |  | Conclusion is not stated | Conclusion is weakly explained. | Conclusion is satisfactorily explained. | Conclusion is well explained. | ____ x 1.25<br>(Max:5) |  |
|  |  | Recommendation is not adequate and irrelevant. | Recommendation is fairly adequate and irrelevant. | Recommendation is adequate and relevant. | Recommendation is adequate and very relevant. | ____ x 1.25<br>(Max:5) |  |
|  | **TOTAL (50 MARKS)** |  |  |  |  |  |  |

## ACKNOWLEDGEMENT

By the name of Allah, the Most Gracious and the Most Merciful,

We would like to thank millions of individuals and organizations for supporting us throughout our degree. First, we would like to thank our supervisor, Dr. Azira Hanani Binti Ab Rahman for her patience, enthusiasm, in-depth comments, invaluable suggestions, useful information, practical advice, and relentless ideas that she has helped us a lot all the time in researching and writing the proposal of this final year research project. Her high knowledge, in - depth experience and professional expertise enabled us to complete this research successfully. We thank her for her invaluable time in guiding us, answering our questions, correcting, and refining the proposal of the final year research project and not forget to thank at our course lecture Cik Siti Fariha binti Muhammad because without relentless guidance and help, this proposal would not have been possible.

We would also like to thank University Malaysia Kelantan (UMK) for the infrastructures and facilities provided by University Malaysia Kelantan (UMK). Without those facilities, we are unable to obtain the sufficient data, journal articles and information required in conducting this research.

We thank the staff and the library of University Malaysia Kelantan (UMK) for organizing various workshops, which have helped me in improving our research and programming skills. This is because on the guidance to provide knowledge and provide relevant education on how to find materials related to our topic to complete the proposal and even his guidance during Covid-19 Pandemic we can learn to some extent to complete this task and even it can help us use it for other assignments.

Finally, we would also like to thank our group members, course mates and parents who always support and motivate us throughout this research. Their dedications are gratefully acknowledged, together with the sincere apologies to those we have inadvertently failed to mention here. Their steadfast support and encouragement are my source of strength.

## TABLE OF CONTENT

# LIST OF TABLES

# LIST OF FIGURES

# CHAPTER 1

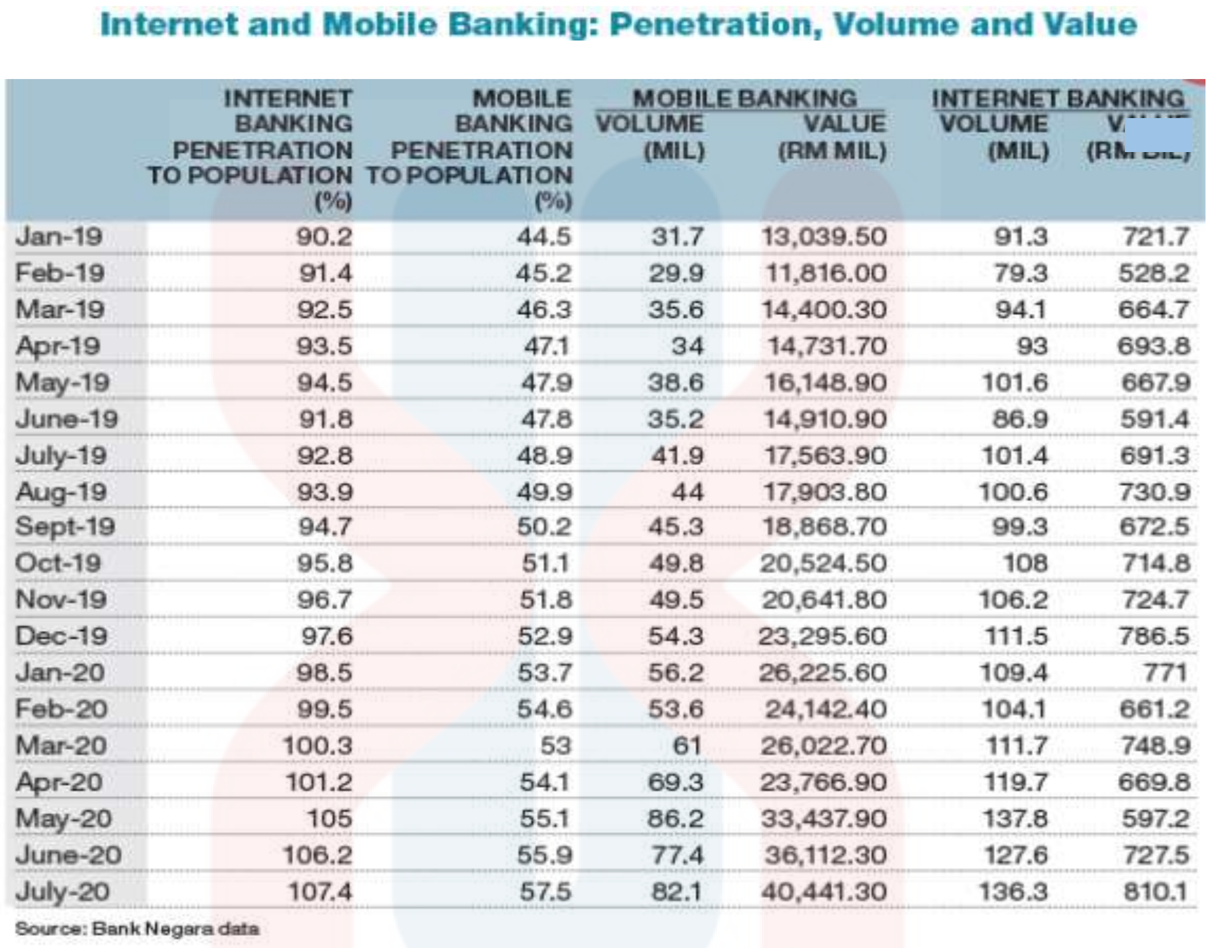
# INTRODUCTION

## 1.1 Background of Study

Internet banking is a system that enables users to conduct standard banking activities such as balance inquiries, money transfers between accounts, and utility bill payment without having to visit a bank (Mahiswaran et al., 2016). According to Rubana et.al. (2016), Malayan Banking Berhad (Maybank) was the first bank to offer online banking services to the public after Bank Negara Malaysia enabled all locally held commercial banks to do so. In Mahiswaran et al. (2010) stated that customers can only use online banking if their bank is registered under the Banking and Financial Institutions Act 1989 (BAFIA) and the Islamic Banking Act 1983. Many other banks have followed Maybank Berhad example in offering online banking services in order to obtain a competitive edge over their competitors and vie for market dominance. The tremendous expansion of online banking use has been fueled by increased deregulation and globalization, as well as considerable impetus for rationalization, consolidation, and a greater focus on costs. As a result, the issue of security safety is critical in warding off internet banking.

Customers are concerned about the security of personal financial information that might be accessible over the Internet. The online banking sector has realized the need of security. One of the most critical elements that influences a customer's decision to utilize online banking is security (Zaiton et al., 2017). As a result, the more internet banking consumers trust in the security of online banking transactions, the more likely they are to utilize the service (Hazwani et al., 2019). To maintain the security of electronic transactions, a number of technologies have been created. In the application of digital certificates and firewalls, the 128-bit RSA (Rivest-Shamir-Adleman) encryption key technology to web browsers is one of the most frequent ways used to safeguard online transactions.

This study can identify the important elements impacting customers adoption of Internet banking. There have been several studies undertaken in Malaysia and other countries that have documented the trend of increasing Internet banking use in Malaysia. Due to security and personal preferences, Internet banking adoption in Malaysia has been gradual (Hema et al., 2017). The biggest barriers to Internet banking adoption in Australia are security concerns and a lack of Internet banking understanding (Yusnorizam et al., 2016). Furthermore, Internet banking customers in Australia were concerned about the safety and security of online transactic However, the security issue in internet banking has not yet been adequately addressed (Omkar et al., 2018). According to Nurhizam et al. (2019), the widespread use of information technology applications connected to e-banking is the key problem for the banking sector. Which results in e-security concerns, cyber-attacks on customers profiles, account hijacking, data message fraud, customer privacy theft, and financial transaction secrecy.



Internet and Mobile Banking: Penetration, Volume and Value

| | INTERNET BANKING PENETRATION TO POPULATION (%) | MOBILE BANKING PENETRATION TO POPULATION (%) | MOBILE BANKING VOLUME (MIL) | MOBILE BANKING VALUE (RM MIL) | INTERNET BANKING VOLUME (MIL) | INTERNET BANKING V[illegible] (RM [illegible]) |
|---|---|---|---|---|---|---|
| Jan-19 | 90.2 | 44.5 | 31.7 | 13,039.50 | 91.3 | 721.7 |
| Feb-19 | 91.4 | 45.2 | 29.9 | 11,816.00 | 79.3 | 528.2 |
| Mar-19 | 92.5 | 46.3 | 35.6 | 14,400.30 | 94.1 | 664.7 |
| Apr-19 | 93.5 | 47.1 | 34 | 14,731.70 | 93 | 693.8 |
| May-19 | 94.5 | 47.9 | 38.6 | 16,148.90 | 101.6 | 667.9 |
| June-19 | 91.8 | 47.8 | 35.2 | 14,910.90 | 86.9 | 591.4 |
| July-19 | 92.8 | 48.9 | 41.9 | 17,563.90 | 101.4 | 691.3 |
| Aug-19 | 93.9 | 49.9 | 44 | 17,903.80 | 100.6 | 730.9 |
| Sept-19 | 94.7 | 50.2 | 45.3 | 18,868.70 | 99.3 | 672.5 |
| Oct-19 | 95.8 | 51.1 | 49.8 | 20,524.50 | 108 | 714.8 |
| Nov-19 | 96.7 | 51.8 | 49.5 | 20,641.80 | 106.2 | 724.7 |
| Dec-19 | 97.6 | 52.9 | 54.3 | 23,295.60 | 111.5 | 786.5 |
| Jan-20 | 98.5 | 53.7 | 56.2 | 26,225.60 | 109.4 | 771 |
| Feb-20 | 99.5 | 54.6 | 53.6 | 24,142.40 | 104.1 | 661.2 |
| Mar-20 | 100.3 | 53 | 61 | 26,022.70 | 111.7 | 748.9 |
| Apr-20 | 101.2 | 54.1 | 69.3 | 23,766.90 | 119.7 | 669.8 |
| May-20 | 105 | 55.1 | 86.2 | 33,437.90 | 137.8 | 597.2 |
| June-20 | 106.2 | 55.9 | 77.4 | 36,112.30 | 127.6 | 727.5 |
| July-20 | 107.4 | 57.5 | 82.1 | 40,441.30 | 136.3 | 810.1 |

Source: Bank Negara data

Figure 1.1: Internet Banking data (January 2019 – July 2020)

Prior to Covid-19 pandemic invading the country in Mac 2020, we can observe that online banking penetration was below 100% and mobile banking penetration was less than 53% of the population. Besides that, the individual online banking members increased to 56.2 million in January 2020, up from 31.7 million in January 2019. This equates to a 9% growth, which is three times the 3% growth seen in the same seven-month period last year. The population's online banking penetration rate increased to 107.4% in July 2020, up from 92.8% in July 2019. Meanwhile, mobile banking's population penetration rate is increasing, while it is still smaller than that of internet banking. The population penetration rate for mobile banking was 57.5% in July 2020. Since March 2020, when it was 53%, it has risen every month. The rate of 57.5% was higher than the 48.9% recorded a year ago in July 2019.

In the meanwhile, data from mobile banking reveals that volume and value have increased at far quicker rates this year. In July 2020, the number of mobile banking transactions reached 82.1 million, up 46 percent from 56.2 million at the start of the year. The value of transactions increased by 54% during the same period, from RM26.22 billion in January 2020 to RM40.44 billion in July 2020. In comparison to the same period last year, these are bigger growth increases. In 2019, the volume climbed by 32% to 41.9 million in July from 31.7 million in January, while the value grew by 35% to RM17.6 billion in July 2019. Intriguingly, the number of mobile banking transactions in July 2020 was 82.1 million, up from 41.9 million in July 2019, while the value of mobile banking transactions was RM40.44 billion, up from RM17.6 billion in July 2019.

Next, data from internet banking shows a similar pattern of expansion in terms of transaction volume and value. In the first seven months of 2020, the number of internet banking transactions increased by 25% to 136.3 million in July. It was also increased 34% year over year (y-o-y) from 101.4 million in July of this year. In July 2020, the value of transactions climbed by 17% year on year to RM810.1 billion, up from RM691.3 billion in July 2019. Cash transactions have decreased as a result of the transition to internet transactions. Malaysians expect cash to account for 72 percent of overall transactions by volume in 2020, down from 93 percent in 2010. According to the Department of Statistics Malaysia (DOSM), the number of households with Internet connectivity has grown to 91.7% in 2020, up from 90.1% in 2019.

Access to mobile phones and computers climbed to 98.6% and 77.6%, respectively in 2020, according to chief statistician Datuk Seri Mohd Uzir Mahidin. According to the Prime Minister's Office's Multimedia Department, a questionnaire conducted during the Covid-19 pandemic revealed that internet usage among Malaysians aged 15 and above climbed dramatically from 84.2% in 2019 to 89.6% in 2020. The use of the internet for services such as education, e-health, e-government, e-commerce, and entertainment had also expanded dramatically. More Malaysians are using the internet to acquire products and services, obtain health information, make online banking transactions, take informal or formal online courses, and obtain information from government agencies, he added. According to Mohd Uzir, the percentage of people ordering products or services through the phone, WhatsApp, or Facebook has climbed from 22.5% in 2019 to 54.4% in 2020.

He stated that during the Covid-19 epidemic, the percentage of Malaysians who used the internet to seek health-related information or services climbed from 45.2% in 2019 to 61.9% in 2020. Meanwhile, internet banking was chosen by 61.9% of Malaysians in 2020, a considerable rise from 50.5% in 2019. In terms of education, the number of people taking informal online courses climbed to 20.8% in 2020, up from 9.5% in 2019, while the number of people attending official online courses climbed to 18% in 2020, up from 8.1% in 2019. In terms of e-commerce, Mohd Uzir stated that the acquisition of products or services through e-commerce platforms like Shoppe, LAZADA, and Grab will climb to 45% in 2020 from 35.2% in 2019. The number of internet users who use e-government platforms to acquire information from government agencies climbed by 7.4% points from 45.5% in 2019 to 52.9% in 2020.

## 1.2 Problem Statement

The Reserve Bank of Malaysia established a "Working Group on Internet Banking" to look at various elements of the technology. The Group concentrated on three primary concerns related to Internet banking: technology and security, legal challenges, and regulator and supervisory concerns. Bank Negara Malaysia has approved the Group's recommendations, which would be implemented in stages.

Banks should also be aware that the original report may provide extensive recommendations on several topics (Syuhaily et al., 2016). In order to gain a high degree of trust from both customers and companies, the Internet must be safe. Authentication, Data Integrity, Confidentiality, Security, and Non-Repudiation are the concerns that will assist maintain a high degree of public confidence in an open network environment. However, there are still hazards associated with Internet banking. Risks linked with Internet banking include credit, interest rate, compliance, liquidity, strategic risk, reputation risk, and foreign currency risk. Due to security and personal preferences, Internet banking adoption in Malaysia has been gradual.

According to Nurhizam et al. (2019), the widespread use of information technology applications connected to e-banking is the key problem for the banking sector. Which results in e-security concerns, cyber-attacks on customers profiles, account hijacking, data message fraud, customer privacy theft, and financial transaction secrecy. The main concerns with Internet banking in Malaysia are a lack of security and the credibility of Internet banking applications. As a result, the purpose of this study is to look at the security factors that determine whether or not people will continue to use Internet banking services.

## 1.3 Research Objectives

The purpose of this study is to empirically investigate the contributing impact of security factor towards internet banking usage in Malaysia.  In order to achieve the aim of this research, the following supporting objectives are established.

i. To examine the relationship between perceived authentication and intention to use internet banking among Malaysia.

ii. To examine the relationship between perceived confidentiality and intention to use internet banking among Malaysia.

iii. To examine the relationship between perceived data integrity and intention to use internet banking among Malaysia.

iv. To examine the relationship between perceived non-repudiation and intention to use internet banking among Malaysia.

## 1.4 Research Questions

The overall research question for this study is what are the impact of security factor towards internet banking usage in Malaysia. To answer the overall question, the formulated research questions for this study are as follow: -

i. Does perceived authentication have a relationship with intention to use internet banking among Malaysian?

ii. Does perceived confidentiality have a relationship with intention to use internet banking among Malaysian?

iii. Does perceived data integrity have a relationship with intention to use internet banking among Malaysian?

iv. Does perceived non-repudiation have a relationship with intention to use internet banking among Malaysian?

## 1.5 Significance of the Study

This study provides one significant insight which is practical perspective. This study is important for society because it will help internet banking users in Malaysia be more cautious about security when conducting online transactions. There are several factors that influence perceived security in online banking transactions, including perceived authentication, confidentiality, data integrity, and non-repudiation. This study will demonstrate that online banking security is linked to customer intention. In Malaysia, the main issues of Internet banking are weak security and the trustworthiness of Internet banking applications. As a result, this study will look into the security factors that impact people's willingness to continue using Internet banking services.

According to the previous study, perceived security relates to consumers' perceptions of the level of security towards Internet banking risks. Customers are more likely to trust Internet banking if they perceive a higher level of security exists. Previous research defined perceived competence as Internet banking users' perceptions of the abilities, skills, and expertise of Internet banking services (Normalini et al., 2019). Internet banking has widely acknowledged the significance and relevance of security issues in customers acceptance of Internet banking, and this has probably advised internet security experts to investigate further on security factors.

The findings of this study have some beneficial ramifications, particularly for the Malaysian banking sector, by providing beneficial insights for increasing online banking security and achieving ongoing usage by the consumer.

## 1.6 Scope of the Study

Empirical investigation is conducted to determine the relationship between perceived authentication, perceived confidentiality, perceived data integrity, perceived non-repudiation and intention to use internet banking among Malaysian. The target population in this study consisted of Internet banking users from Malaysia. The sampling frame for this study is among aged 18 until 50 years Malaysian users and the sampling method was applied in this study is limited to particular groups of persons who can offer the needed information, namely are Internet banking users. This study will accomplish in examine consumer intention that related to security factors in the use of internet banking and how this practice affects internet banking users. This study adopts with the theory of Technology Acceptance Model and Model of Trust. Recognizing that there are many categories of perceived security variables that banking institutions should be able to do in order to improve security, this study will mainly focus on online banking security as one of the aspects of customer intentions in the use of online banking.

## 1.7 Organisation of Chapters

This research is divided into five chapters. The research context is covered in Chapter 1, where it discusses internet banking and the issues that are relevant to this study. Additionally, in this chapter also provide a brief description of security on internet banking, intention and what factors influence customer's intention in Malaysia. Furthermore, it also provides an explanation on the significance of customer's intention of using internet banking. The problem statement, research objectives, research questions as well as the significance and scope of the study is also discussed in Chapter One.

To provide a more detailed explanation of the security of e-banking use and the variables that drive customers to use e-banking in Malaysia, Chapter 2 explains the relationships and brief explanations that was utilized in this study which is intention, perceived authentication, perceived confidentiality, perceived data integrity, and perceived non-repudiation. The theoretical framework and other related theories in this study are also presented in Chapter Two. Each variable of the factor was discussed in context of internet banking and how it is likely to influence consumer intention to use e-banking in Malaysia.

Next, Chapter 3 discusses research methods including the research design, measurement development, size of the study, population, unit analysis, sample and sampling method, and data collection techniques. The software that will be used for data analysis is SPSS and it will be discussed in detail in this chapter.

The analytical processes required as well as the study's findings covered in Chapter 4. Elements such as demographic information and statistical results from data analysis were provided.

Lastly, Chapter 5 discusses data analysis and summarises the findings and conclusions. This chapter also explored the implications of the findings, the study's limitations, and future research ideas.

## 1.8 Operational Definitions

| Term | Definitions | Sources |
|---|---|---|
| Intention | Measures a person's relative strength of intention to display a specific behaviour. | Adopted from (Normalini et al., 2019) |
| Perceived Authentication | The process through which an Internet merchant can be established via a trusted third party that guarantees that the merchant is indeed who they say they are and it also ensures that the trading parties in an electronic transaction or communication are who they claim to be. | Adopted from (Normalini et al., 2019) |
| Perceived Confidentiality | Confidentiality warrants that all communications between trading parties are restricted to the parties involved in the transaction. | Adopted from (Normalini et al., 2019) |
| Perceived Data Integrity | Data in transmissions are not created, intercepted, modified or deleted illicitly. | Adopted from (Suh & Han et al., 2003) |
| Perceived Non-Repudiation | Mechanism to ensure that the customers can be certain they are communicating with the genuine server (bank), or vice versa, such that neither of the communicating parties can later falsely deny that the transaction took place. | Adopted from (Normalini et al., 2019) |

# CHAPTER 2

# LITERATURE REVIEW

## 2.1 Introduction

This chapter will be describing the relevant review of research studies on the security factors influence behavioral intentions towards e-banking usage in Malaysia. Moreover, this chapter will be present a definition of the dependent variable and independent variable. This part gives a superior understanding with respect to the advancement of the research framework including the dependent variable (behavioral intention) and the independent variables (perceived authentication, perceived confidentiality, perceived data integrity and perceived non repudiation). In general, two theories are employed to explain the observations in this study: Technology Acceptance Model (TAM) and Model of Trust. Some factors from earlier research were deemed to be appropriate for this study's framework and objectives. This chapter concludes with a description of the suggested conceptual framework and its characteristics.

## 2.2 Theoretical Framework

### 2.2.1 Technology acceptance model (TAM)

The technology acceptance model (TAM) is an information systems theory that explains on how consumers learn to accept and use a technology, according to Davis et al. (1989), the originator of TAM. The end-point where humans use technology is the actual system utilisation. TAM2 is a semi-developed TAM model that depicts perceived usefulness constructs such as subjective norm, image, and work relevance. These sorts of constructions show that people who embrace or reject a new technology will find it more beneficial. The extra constructs in TAM3, which is more developed than TAM2, demonstrate how new technology can make life easier for individuals.

This created approach should be implemented in other domains where technology is used, such as transportation, urban planning, and infrastructure management. The development of TAM3 models would offer a solid foundation for decision-makers and managers in a variety of domains. The notion that utilising Internet Banking would increase one's efficiency is known as perceived usefulness (PU), whereas the opinion that using Internet Banking would be painless is known as perceived ease of use (PEOU) (Davis, 1989). External factors like preparation and technology characteristics have an impact on behavioural purpose and usage, but PU and PEOU mediate it.

PEOU has an effect on PU because, all other aspects being similar, the better a technology is to use, the more efficient it can be. TAM also shows that PEOU's causal impact on behavioural intention is only important early in its use (Normalini et al., 2017). As user interface grows, this influence becomes indirect and works by PU in the long run (Bestoon et al., 2019). Because there is a scarcity of information on the impact of PEOU on intentions and behaviour, PEOU and Perceived Behavioral Control (PBC) (measured by self-efficacy and controllability) were combined into a single composite component termed perceived manageability, which assessed customers' perceptions of internal and external obstacles to using Internet Banking systems (Viknesh et al., 2017).

TAM is the most commonly used paradigm for researching Internet banking behaviour. According Normalini et al. (2019), model replication TAM constructs PU and PEOU have theoretical underpinnings and model replication in the Internet Banking sense have been the subject of previous TAM studies. Modification of the model by combining TAM with other models, as well as model extension by including external structures as direct predictors of mood, intents, or usage (Viknesh et al., 2017). The core benefits of TAM, such as parsimony and a utilitarian and technical orientation, will make it easy to underestimate the impact of a customer's social and psychological views on technology acceptance. TAM has also been chastised for failing to recognise human distinctions (Kritika Law et al., 1999). The original TAM overlooks elements like prior experience, age, gender, and a plethora of other human traits that might influence attitudes toward technology and, as a result, the motivation to utilise it.

To overcome these constraints, other research incorporated variables as antecedents, covariates, or outcomes of TAM. Zaiton et al. (2017) applied ‘perceived tools' to TAM based on Theory Planned Behaviour’s (TPB) build Perceived Behaviour Control (PBC). Perceived resources are described as the extent to which an individual believes he or she possesses the personal and organisational resources necessary to employ a technology, such as expertise, hardware, software, assets, paperwork, records, human support, and time. TAM's predictive ability in terms of mobile banking uptake was considerably boosted by integrating perceived cost, self-efficacy, and perceived repute (Viknesh et al., 2017). However, there is inconsistent evidence on this issue, with indicating that apparent cost had no effect on behavioural intention to utilize mobile banking (Mahiswaran et al., 2016). Identifying and theorising social influence (SN and Image) as drivers of PU, as well as cognitive instrumental processes (job significance, performance efficiency, outcome demonstrability, and PEOU), Mathavi and Dineswary (2017) identifies and theorises social impact (SN and Image) and cognitive instrumental processes (job relevance, output quality, result demonstrability, and PEOU) as drivers of PU, resulting in TAM2 (TAM2). They have added insight and willfulness to the current worldview as mediators. Mathavi et al. (2017) proposed computer fear, enabling circumstances, computer playfulness, and computer self-efficacy as factors of PEOU in a similar vein. TAM3 is an improved TAM model created by combining TAM2 (Mathavi et al., 2017; Dineswary et al., 2017). TAM3 is the most stable variation of TAM, however no study has been done to put it to the test in the field of Internet banking.

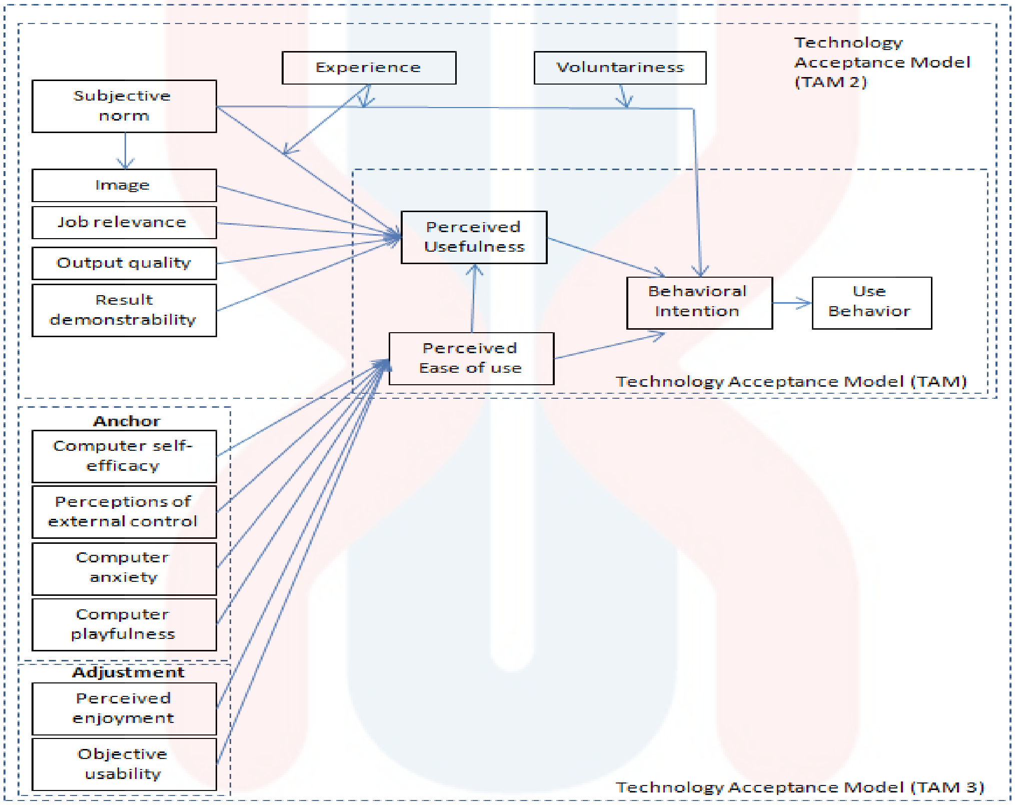


Figure 2.1: Technology Acceptance Model (TAM, TAM2 and TAM3)

Sources: Davis (1989)

### 2.2.2 Model of Trust

The electronic banking industry has recognised consumer trust as a key aspect. Because of the unpredictable existence of the online world, factors that impact trust and its growth differ from those that affect conventional banking services. Security plays an important role in the formation of confidence, according to extensive research into the factors that influence it. One or more authentication procedures secure users' online banking practises at all times. Analysing the impact of these processes on the construction of a user’s impression of security, as well as the impacts of that discernment on trust, is one technique to look at the role of security in trust formation.

One of the most significant problems facing the market, as in most other e-commerce sectors, is a lack of consumer confidence (Normalini et al., 2019). According to Kritika et al. (2017), confidence is a critical component in accelerating the growth of online apps. Uncertainty, secrecy, and opportunities for individuals to take unfair advantage of the scheme characterise internet-based purchases (Kritika et al., 2017). Because of the unpredictability and unreliability of the underlying network, trust is a critical component throughout this setting. Most other electronic networks, such as the smartphone environment, have a lower risk perception than the internet (Kritika et al., 2017). Understanding the nature of consumer confidence, as well as the elements that drive it, can aid you in predicting how it will develop.

Several features associated with the website are used to create confidence, including architecture, navigation, information, protection, usability, and so on. One of the most significant features that affect user loyalty is the security protocols used by websites, revealed that in a physical banking setting, the consumer's protection and privacy are quite important (Normalini et al., 2019). As a result, security and anonymity are crucial in creating confidence in virtual banking.

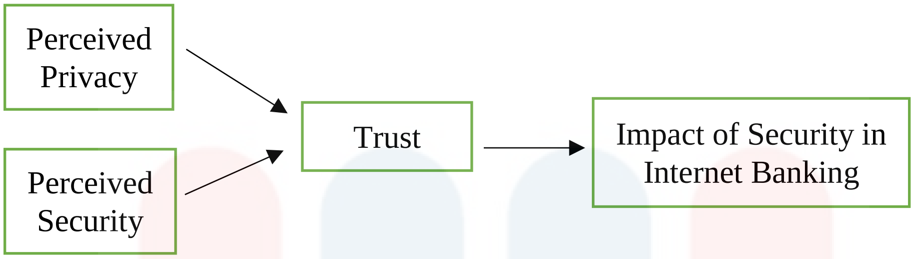


Figure 2.2: Model of Trust (Kritika, 2017)

## 2.3 Previous Empirical Studies

### 2.3.1 Intention to use E-Banking

Behavioral intention assesses a person's willingness to engage in a given behaviour. If an individual wants to do something, it is more likely that customer does it. This implies that customers' behavioral intentions (BI) to continue utilizing web banking can decidedly affect how they draw in with internet banking system. Intention is portrayed as the power of an individual's longing to take part in a particular conduct. The core element in TPB and TAM is an individual's desire, as both hypotheses posit that action is dictated by the intention to execute the behaviour.

Customers' decisions and preferences to remain or move from company offerings are influenced by behavioural intention (Zeithaml et al., 1996). Customer perception, according to Zhang et al. (2005), is more closely linked to behavioural motive. It is said that the more favourable a customer's experience is, the more likely they are to choose to purchase or use the services. However, the desire to use e-banking services is determined by a variety of reasons, each of which has a different effect on usage. Consumer willingness and propensity to use a particular piece of technology are characterised as behaviour purpose. Through the widespread use of smartphones, cellular mobile services have been embedded into consumers' lives, implying that they are able or expect to use mobile phones to conduct e-banking transactions. The only dependent variable in this study is behaviour intention. Prior research has distinguished various elements that may impact behaviour intention, including perceived ease of use, social effect, and mobilisation.

Many scholars around the world have recently focused on explaining and forecasting consumer intentions and internet banking acceptance, and the applicable literature related to online banking platforms has seen a drastic increase in this field (Lin et al., 2011; Purwanegara et al., 2014; Zhou et al., 2012). Several hypotheses aimed at explaining and predicting the interaction between consumer expectations, behaviours, and the intention to utilise technology in a particular way have arisen in recent years (Oruç et al., 2017). The TAM has been shown to be a reliable hypothesis for predicting implementation activity and behavioural intention, with the most important factors of emerging technology acceptance being perceived utility and perceived ease of use.

Behavioural intention refers to an individual's conscious decision to utilise or not use Internet banking (Kao Huang et al., 2015). Behavioral intention has been demonstrated in several earlier research plays a significant role in real usage behaviour. For example, Omotayo et al. (2015) investigated the factors affecting postgraduate students at the University of Ibadan in Nigeria's plan to use internet banking. The study embraced the Technology Acceptance Model and Theory of Planned Behavior as the theoretical framework. The consequences of the study uncover no huge connection between demographic characteristics and intention to adopt internet banking, while the individual variables and social factor altogether affected intention to adoption internet banking.

Then again, Khan, et al. (2017) inspect the variables prompting customers' intention to utilize E-banking administrations in Malaysia. Customers' intentions to use E-banking services in

Malaysia are significantly influenced by comfort, confidence, perceived ease of use, and perceived utility, according to the findings. Mazuri et al. (2017) investigate the reasons that affect Pakistani customers' plans to utilize web banking in an alternate setting. Perceived utility, perceived ease of use, and attitude were discovered to be the main builds for advancing web banking use in Pakistan. Moreover, the worth yields framework audit uncovered that the main perspective was attitude. As a result, banks will concentrate on cultivating favourable attitudes toward internet banking among potential customers.

The factors that affect customers' willingness to engage in e-banking transactions through cell phones in a different context. The findings showed that perceived compatibility and versatility have a significant impact on perceived usability, and that perceived usefulness fundamentally affects intention when it comes to using e-banking on mobile devices (Shiqian et al., 2018). It looked at perceived utility as a mediator between perceived compatibility and behaviour intention, as well as versatility and behaviour intention. The security factors that influence customers' eagerness to utilize Internet banking in Malaysia (Normalini et al., 2019). The discoveries propose that customers' impression of confirmation, secrecy, and information protection both assume a part in their choice to keep utilizing Internet banking. Perceived non-repudiation, then again, affected the choice to keep utilizing Internet banking in Malaysia.

Understanding the components found in this study would permit Internet banking suppliers to rapidly and effectively improve administration assurance, subsequently reassuring shoppers to keep utilizing Internet banking. The point of this study is to view at potential security contemplations as multidimensional form impacts on the arrangement to utilize Internet banking later on. More recently, the factors influencing the behavioural intention to adopt mobile banking among Universiti Putra Malaysia students has been conducted by Osman et al. (2020). The results then revealed that performance expectancy, habit, and perceived reputation were all important predictors of behavioural intention among students, with performance expectancy being the most significant. As a result, the study's results have many consequences that would be useful to service providers, banks, and potential scholars.

An extended model to foresee and clarify customers conduct expectation as to receiving web-based banking has been introduced (Al-Gharaibah et al., 2020). To have a more detailed inquiry into online banking, the suggested model combines four variables. In Malaysia, data was gathered from graduate students. The proposed model has modest explanatory capacity, according to the findings. Furthermore, the effects of ease of use and consumer attitude are strongly linked to E-Banking acceptance. In comparison, perceived utility and vulnerability have no major relationship with E-banking adoption. Decision makers must ensure that E-banking is simple to use and that specific instructions are given for accessing the services.

### 2.3.2 Perceived Authentication

Customers' trust in utilising internet banking would rise if they were subject to security procedures such as authentication, fingerprints, response connections, encrypting, message authentication, screening firewalls, password management, hardware compatibility security, and card readers. (Yousafzai et al., 2003). Grandinetti et al. (1996) characterised security as the technological assurance that legal and ethical standards be followed, while Casaló et al. (2007) defined security as the protection of data from unauthorised persons. Aladwani et al. (2001), and Jun et al. (2001) discovered that, because of the lack of personal contact, IT directors and purchasers were more worried about the security of web-based banking than they were about the security of traditional banking.

Users' complaints regarding security mechanisms ensuring anonymity, clearance, authentication, affordability, non-repudiation, and fraud prevention are referred to as "Internet banking security concerns." The first topic to consider in online transactions is protection, which is regarded as a necessary component of trust. Consumers using Internet banking must feel safe when providing personal information, credit card numbers, and other sensitive information. As a result, one of the most important conditions for trust is stability. Electronic banking (or e-banking) has grown rapidly in Malaysia in recent years, according to Zaiton et al. (2017) it revolutionises conventional banking services and causes a significant change in the field of international marketing strategies. Despite its widespread use, a large number of customers remain sceptical of its efficacy and performance. All independent variables, with the exception of adequate framework, were found to be significantly linked to the perception of e-banking protection.

Authentication is a method in which users must affirm their identities by completing a validation process. The two major components of network stability, anonymity and authentication (Yang et al., 1999). User authentication is used to "confirm a human user's assumed identity" (Monrose et al., 2005). The authentication mechanism consists of three security components that fluctuate among approved and unapproved customer: mystery, which guarantees that data is blocked off to unapproved customer, straightforwardness, which guarantees that information has not been adjusted in an unapproved way, and convenience, which guarantees that computer systems are open to approved parties as required (Braz et al., 2005).

In banking, confirming the legitimacy of a contact, purchase, or access request is critical. As a result, banks can use dependable methods to validate new consumer identification and authorization, just as to verify the personality and approval of existing customer endeavoring to start electronic exchanges. In a completely electronic open organization climate, setting up and confirming a person's personality and consent to enter banking organizations can be troublesome. A host of "spoofing" methods may be used to misinterpret legitimate user authorization. A sense of confidence when doing online purchases is considered a crucial element in removing consumer anxiety. According to Salisbury et al. (2001) a sense of protection when doing online transactions is a crucial aspect that alleviates consumer worries over online purchases. Customers are more likely to use e-services if they believe their purchases are safe (Cheng et al., 2006).

Clearly security affects the utilization of e-banking administrations, with higher security prompting expanded use. Therefore, there is hypothetical and observational proof of a generous connection among trust and e-banking reason. One of the most critical factors that affects consumer acceptance is stability (Daniel et al., 1999). It can be inferred that consumer will not use e-banking services unless they believe they are stable. When looked at the relationship between perceived security and confidence, she discovered that perceived security had no effect on trust (Kritika Law et al., 2007). This finding indicates that, while security function indicators have a significant effect on security perception, the insight that they encourage doesn't assume a critical part in developing trust. At the point when the entirety of the individual sections of apparent secrecy were inspected, it was found that protection translation has a considerable beneficial outcome on certainty. As a result, improving this aspect of understanding will aid in the attempt to increase customer interest in online banking.

Nonetheless, Al-Sharafi et al. (2016), contend the inquiry: 'Do security and protection insights influence customer trust to acknowledge and utilize Internet banking innovation to play out their financial exchanges?' The variables that affected Jordanian customer ability to consider Internet banking administrations were explored in this report. The findings indicated that the proposed model accurately reflected the variables that influence interest in accepting and using

Internet banking services. The findings revealed that confidence has a positive impact on behavioural intention to use Internet banking services, with perceived utility, protection, and privacy both influencing perceived trust. Finally, perceived ease of use did not forecast Jordanians' willingness to use online banking.

Thus, according to Normalini et al. (2017), internet banking is getting more normal in Malaysia because of its accommodation, which is accomplished by means of explicit business communications between banking establishments and customers through websites and mobile applications. In any case, the extraordinary ascent in web extortion cases has put web banking customer security and privacy in danger. This research sheds light on the potential for biometrics technologies to be used in internet banking to ease privacy and security issues while also increasing confidence among Malaysian customers.

While there was no substantial interaction between perceived privacy and confidence, the results showed that perceived biometrics efficacy strongly affected the intensity of the relationships between perceived privacy and perceived protection with trust. (Renaud et al., 2005) portrayed three phases of validation: ID, authentication, and authorisation:

1. The mechanism by which the device begins to recognise the user's identity and determine who they are is known as user identification. Users typically enter a name or identity code during this step, and the machine matches the database with the text. However, since user authentication is inadequate, the following two steps are needed.

2. The key method for confirming a user's identity is user authentication. During this point, the user must have a hidden element, such as a password, protected response, or a number, which must fit the one allocated to the user in their record.

3. Application authorisation gives the user admittance to the scrambled site, which must be accomplished after the initial two stages have been finished effectively.

Ahasanul et al. (2009) investigated online customers' views of electronic transactions and found that considerations such as safe transactions, adequate mechanisms, service efficiency, and regulatory structure all play a role in how they perceive e-banking transactions. Only the encrypted transaction was found to have a substantial impact on consumers' perceptions of e-banking in their report, whilst the other three aspects did not. First and foremost, in e-banking, cyber security is a consistent and basic need for bankers (McCahon et al., 1999; Haridaet al., 2000). It is clarified as a "interaction used to ensure a data system, or a danger the board or hazard alleviation apparatus". (Ahasanul et al., 2009). High security covers both delicate and hard framework that shields customer data from programmers (Glaessne et al., 2002). Specifically, the delicate system is comprised of strategies, cycles, conventions and rules that ensure the system and the information; while hard foundation comprises of equipment and programming expected to shield the system and information from dangers.

According to Chellappa et al. (2002) as quoted by Ahasanul et al. (2009), at the point when all data associated with an exchange is "began by the right element and enters the planned party without being noticed, changed, or lost during transport and capacity", it is called a protected transaction. Consumers' perceptions of security are shaped by "visible appropriate measures that are implemented by encryption, protection, verification, and authentication processes." To maintain service security, utilizing encoded or decoded information that must be deciphered by the sender and beneficiary (Michel et al., 2003).

### 2.3.3 Perceived Confidentiality

The term "confidentiality" is employed to avoid data leak to unapproved elements, people or cycles. It alludes to security touchy and important property from unapproved revelation or block attempt. Privacy likewise implies that solitary verified gatherings or frameworks have the position to get to put away information. Information privacy could be penetrated either purposefully or inadvertently in various manners including hacking, phishing, email ridiculing and sending malignant code through email or both organizations.

This is to ensure that communication between users or customers and service providers cannot be intruded or accessed by other parties (Suh et al., 2003). Getting to others' data without consent ought to be forestalled promptly (Knorr et al., 2000). This should cover both the classification of data conveyed over the organization and the mystery of data kept in different spots (Maijala et al., 2004).

All correspondences between exchanging parties are limited to the gatherings engaged with the exchange, as indicated by confidentiality. Since programmers may access one's delicate data, confidentiality is critical in the e-commerce world. As a result, a bank's website should provide financial confidentiality (Sobihah et al., 2015). While expanding by and large security is basic for electronic frameworks, dissecting security as far as destinations like confidentiality, authentication, and so on can help customers acquire a superior comprehension of the objectives that are generally critical to them. As indicated by Chellappa et al. (2002), upgrading this agreement is basic for the drawn-out feasibility of electronic applications.

The objective of this study is to get familiar with the idea of the connection among trust and security, two of the main obstructions in electronic banking and other online business applications. Studying their relationship and the impact of safety on trust would be useful in fortifying these endeavors, as persistent innovative work is in progress to improve internet business security and trust building measures. The investigation by Sarrafiaghdam et al. (2003) show that confidentiality is a huge indicator to the apparent data security and he accepted that there were fits among privacy and data security for the customer to be persuade in utilizing web banking system. It is important for keeping up the privacy of the individual data against unapproved perusing, duplicating, or exposure utilizing encryption components (Ratnasingam et al., 2002).

Yousafzai reviewed the elements influencing customer trust in e-banking and proposed a model. This model depends on two components: perceived security and perceived confidentiality. Obviously, the acknowledged components by bank frameworks including consideration, trustworthiness, and skill positively affect two primary variables in certainty building; therefore, driving customer to use E-banking administration (Yousafzai et al., 2003).

### 2.3.4 Perceived Data Integrity

Integrity is one of the critical parts of data security and alludes to information, programming and equipment. It implies that resources are modifiable just by approved gatherings. Information honesty shows shielding information from unapproved activities like change and creation. Truth be told, respectability empowers us to perceive any performed adjustment and control of information (counting addition, erasure and replacement) by unapproved substances. Bank customers should be sure about newness and validity of got data. Information honesty guarantees the precision and fulfillment of data in the capacity and change status. It is abused when a substance erases or changes significant information records whether coincidentally or malevolently.

Data integrity alludes to the shortfall of unapproved advancement, interference, change, or cancellation of information in transmissions (Suh et al., 2003). To guarantee the protection, privacy, and honesty of exchanges and data that is traded, uncovered, sent, put away, or utilized in internet banking frameworks, banks utilize a mix of validation, encryption, and inspecting components. The mix of these strategies makes an amazing hindrance to forestall framework passage and maltreatment in any way.

During and after the exchange of information, the content ought to remain unchanged and free from interference. On the off chance that this happens it will make harm the data information accidentally and purposefully (Grandison et al., 2000). Toleman et al. (2005) argue that the trustworthiness of the set-up state is to guarantee that messages are not made, adjusted, caught or erased by unapproved people. As per Ally et al. (2005), Kesh et al. (2002) and Maijala et al. (2004), every security component utilized is to meet explicit security purposes like confidentiality, integrity, etc. A progression of autonomous security reviews is performed to confirm that all cycles are consistently checked to guard and protect against known security issues, just as to keep away from any sort of altering, information robbery, or exchange chances.

The investigation expressed by McKnight et al. (2002) integrity is the consumer’s conviction that a trustee's responsibility in offering types of assistance is straightforward, moral and should be satisfied. The consumer’s conviction that the substance conveying the assistance isn't abusing them and really needs to convey the help is known as consideration. Every one of these dimensional highlights doesn't characterize a part of trust yet they establish the framework and lead to the extension of trust.

Sarrafiaghdam et al. (2003) led an overview on 132 respondents in Klang Valley. In light of the measurable investigation, they found that uprightness is a significant component in the web banking framework that should be set up to cultivate the security framework. Integrity is disregarded when a message is effectively changed on the way. Data security frameworks commonly give message trustworthiness notwithstanding information privacy. In this manner, customers depend on the integrity of such framework in doing exchange by means of web banking.

### 2.3.5 Perceived Non-Repudiation

Non-repudiation is a feature that ensures customers that they are communicating with a genuine person (bank), or the other way around, to such an extent that neither of the conveying gatherings can later dishonestly reject that the exchange occurred. Banks maintain and regularly update exchange logs, which contain a variety of information such as the nature, time, and date of customers transactions. These records allow for the verification of all sorts of transactions done and offer the necessary documentation in the event of a problem.

The point of this is to guarantee that the gathering associated with starting an exchange, sending any data, or accepting any data can't keep it at a later case from getting time (Ally et al., 2005; Kesh et al., 2002; Maijala et al., 2004). The elaborate members in a specific exchange won't deny their exercises during a specific exchange, related data ought to have recorded. Security insurance: Privacy assurance is to defend the recognizable data (PII). Every one of the elaborate members should just know his ideal data. Merchant should know just request of merchandise subtleties, not the customers card number, covered up number, ledger. Bank should realize just customers buy affirmation, ledger, and sum to be dispensed. Also, an untouchable should not have the option to intrude, reconnaissance or delivery any data in regards to the exchanges.

Due to increased customer demand for data access, the number of security measures will constantly rise. Sung S. Kim et al. (2011) stated that to improve security in online banking services, a number security measures have been examined, including authentication, privacy, and non-repudiation. To lead a better security, various techniques of security can be used in implementation of these types of security controls.

## 2.4 Research Framework

The study framework is based on the impact of security on Internet Banking Usage Intention among Malaysians, and it includes four intention variables, which are perceived authentication, perceived confidentiality, perceived data integrity and perceived non-Repudiation. Four hypotheses were suggested to test the framework in order to determine the link between security variables and the desire to continue using Internet banking.

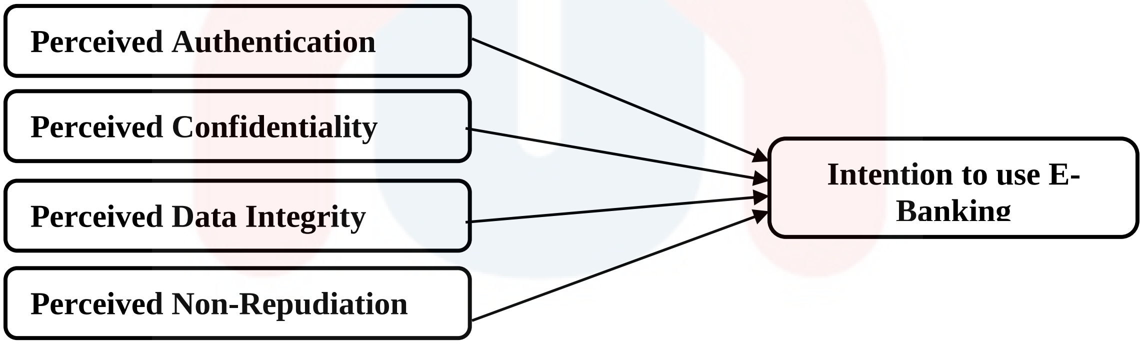

Perceived Authentication
Perceived Confidentiality
Perceived Data Integrity
Perceived Non-Repudiation
Intention to use E-Banking

Figure 2.3: Research Framework

## 2.5 Hypotheses Development

As indicated in Figure 2.3, the research hypotheses employed in this study were generated for the research aims and framework. To support the proposed hypothesis, past empirical evidence on relationships between variables are provided. The theories offered are specifically geared at providing solutions to the research problems raised throughout this study.

### 2.5.1 Relationship of E-banking usage intention and perceived authentication

The previous research applied the Technology Acceptance Model (TAM) framework in the field of e-commerce to demonstrate that consumer interest in e-commerce can be greatly predicted by their intention to participate in online transactions. While attitude is a predictor of intention in the original TAM model, confidence is a better predictor of intention. Customers would not use internet banking if they did not have interest in financial institutions (Normalini et al., 2019). Internet Banking is a method that enables consumers to manage banking transactions securely through any system that has access to the internet. Almost all transactions in a branch are included, such as money transfers, account opening, insurance transactions, loan applications, and so on (Hazwani et al., 2019). Several other security factors, such as authentication and authorization have been established and integrated into the security system.

According to a prior study, perceived usefulness and ease of use, risk in online banking, and personal IT innovation all affect online banking use favourably. However, in order to investigate factors impacting online banking adoption, the Technology Acceptance Model (TAM) is being used. As a result, perceived benefits attitude and perceived usefulness have a favourable impact on an intention to use internet banking, but protection and privacy issues, as well as financial risk, have a negative impact (Aminul Islam et al., 2015). Following that, Zaiton Osman et al. (2015) noted that consumers' trust in the website drove user intent, and that transaction security, as well as website and company expertise, affected trust effectively and cognitively. Consumers' impression of safety is regularly molded by apparent adequate systems completed by cycles of encryption, guard, check, and validation. The user or device should demonstrate its personality to the customer during confirmation. Commonly, server confirmation requires the utilization of a username and secret phrase. For instance, cards, eye checks, discourse acknowledgment, fingerprints and different strategies for validation.

However, authentication does not decide which functions an individual can perform or which data each person can access. Authentication simply defines and verifies the identity of the individual or device. Recent internet banking studies have generally acknowledged the position and relevance of security risks in consumer acceptance of Internet banking, and have perhaps cautioned internet security researchers to investigate further on security dimensions. However, no consideration was paid to empirically investigating security issues. The previous study used a model that combines the key security aspects to define variables that affect the decision to continue to use Internet banking including perceived authentication. As a result, it is hypothesis that when appropriate tools are available and made known to their customers, consumers will view e-banking as more stable.

**H1: There is a significant positive relationship between E-banking usage intention and perceived authentication.**

### 2.5.2 Relationship of E-banking usage intention and perceived confidentiality

The TAM paradigm focuses on how something is thought to be used. Chipboards and fires will scatter the latest wave of plastic cards in Hungary. The banks will be the primary consumers of chip cards, as they will need their success first and foremost. You may even verify the identification of your personal and ad on smart cards without jeopardising the user's partnership with the bank's confidentiality (Amran Harun et al., 2019).

Perceived security had little impact on trust when she investigated the connection between perceived security and confidence (Kritika Law et al., 2007). This result suggests that, while security feature indicators have a strong influence on security perception, the perception that they cultivate doesn't even have a significant impact on confidence cultivation. Privacy perception has a significant beneficial impact on trust as all of the individual elements of perceived confidentiality are tested. As a result, increasing consumer participation in online banking can be aided by strengthening this aspect of comprehension. In the previous s study that the confidentiality was found to have a substantial positive influence on consumers' intention to continue to use online banking (Normalini et al., 2019). It could be inferred that confidentiality can aid in the creation of long-term use of internet banking because banking typically necessitates accurate information. According to the findings, confidence has a positive effect on the intention to use online banking services with perceived utility, security, and privacy both affecting perceived trust.

According to the previous study, confidentiality requires that all transactions between trade partners be limited to those interested in the exchange. Since hackers can access sensitive information, confidentiality is extremely essential in the e-commerce environment. Banks utilize a mix of confirmation, security, and evaluating cycles to guarantee the mystery, classification, and believability of exchanges and data traded, uncovered, posted, saved, or utilized in web based financial frameworks. Notwithstanding, the scope of free security evaluations are needed to guarantee that the all systems are consistently tried to get and shield against set up security issues and to dissuade any sort of altering, misrepresentation, or danger to exchanges (Normalini et al., 2019).

**H2: There is a significant positive relationship between E-banking usage intention and perceived confidentiality.**

### 2.5.3 Relationship of E-banking usage intention and perceived data integrity

The Technology Acceptance Model has been shown to be a legitimate theory that gauges selection movement and social reason with an emphasis on perceived utility and perceived ease of use as the main drivers of new technology acceptance. This model (Technology Acceptance Model) is similar to our variable, which is the factors of security in internet banking that can affect customer intentions.

The previous study supported the critical importance of data privacy as a major predictor of consumers' intent to continue using Internet banking. As a result, data integrity may encourage the continued use of Internet banking because data in transmissions is not generated, captured, changed, or removed illegally. The logical rationale for this conclusion may be that if Internet banking customers in Malaysia have trust in the efficiency of Internet banking, they will feel more comfortable performing banking transactions electronically using Internet banking. In addition, perceived data integrity was the most important indicator of Intention, followed by perceived authentication and perceived confidentiality which is indicating that Malaysian Internet banking users are very concerned with data integrity (Normalini et al., 2019).

Next, Zaiton Osman et al. (2015) stated that high protection encompasses both hard or soft networks and shielding consumer data from hackers. The soft infrastructure, in particular, consists of rules, procedures, conventions, and guidelines that ensure the framework and information, while the hard foundation administrations containing the software and hardware can secure the information and data from attacks. A stable transaction happens since all data involved originates from the correct entity. The more secure the exchange, the more secure customers would feel about E-banking transactions. This past statement showed that the perceived data has a positive correlation with the consumer's intention of using the internet banking. All users will feel safe when using online transactions because their data was stored securely.

**H3: There is a significant positive relationship between E-banking usage intention and perceived data integrity**

### 2.5.4 Relationship of E-Banking usage intention and perceived non-repudiation

According to the past study, the purpose of this variable which is non-repudiation is to guarantee that the individual engaged with leading an agreement, communicating data, or getting data can't dismiss it at a later stage.

Past study has tracked down that perceived non-repudiation marginally affects consumers' intentions to keep utilizing web banking. Past study results may have been slanted by the area chose for empirical investigation, and web banking customers in Malaysia may feel that different concerns like authentication and data integrity are more relevant. Accordingly, from the past study on it was expressed that it is feasible to contend that the irrelevant effect of perceived non-repudiation on customers intention to keep utilizing Internet banking which can be clarified by two components. To start with, perceived non-repudiation won't be viewed as a critical issue, bringing about a low nearer valuation. Second, respondents' comprehension of alleged non-repudiation is lacking. These non-repudiation documents accommodate the confirmation of all types of executed exchanges and incorporate the proof required if an issue emerges (Normalini et al., 2019). Consumers may feel more secure transacting knowing that one entity which is the seller cannot cancel the transaction (Syaiful Ali et al., 2021). The inclusion of a non-repudiation pledge is expected to improve the sense of security associated with online transactions. A digital signature is among the most often used authentication measures for ensuring non-repudiation.

However, the previous study also stated that non-repudiation has been shown to be one of the most important aspects of perceived security (Turban et al., 2010). It concerns the transaction between of buyers and sellers, specifically the system's ability to ensure that the individual claiming to be the seller obtained details submitted by the buyer. Nonrepudiation means that the vendor cannot dispute the fulfilment of the contract (Siponen et al., 2007). These findings showed that the perceived non-repudiation was correlated positively with perceived security in the previous study.

The essence of their interaction was established when developing a model of the relationship between trust and security (Normalini et al., 2019). To begin, the existence of security mechanisms is thought to have a positive effect on security perception. Second, an improvement in customers' understanding of protection is said to have raised their level of confidence. Subsequently, protection assumes a significant part in the formation of trust among E-banking customers. The records of apparent security have an enormous load on the parts of apparent security with which they are associated. The past investigation's measurements mirrored the translation of protection relying upon the security measures that impact it. In view of these assertions, it is feasible to gather that protection measures such as confidentiality, authentication, integrity, non-repudiation, and so on profoundly affect the comprehension of security. It is additionally expressed that the presence of safety components positively affects security insight.

**H4: There is a significant positive relationship between E-Banking usage intention and perceived non-repudiation**

## 2.6 Summary of the chapter

This chapter discussed the overview of e-banking industry and the literature relating to the study variables. The underlying theories such as Technology Acceptance Model (TAM) and Model of Trust that clarified the measure factors in this research were considered and appropriately talked about. Based on these theories and literatures, the research framework for this study for this investigation has been detailed and introduced. Finally, the study hypotheses were postulated. The proposed hypotheses in this study are summed up in Table 2.2.

Table 2.1: The proposed hypotheses.

| No | Hypotheses | Statement |
|---|---|---|
| 1. | H1 | Perceived authentication has a positive relationship with e-banking usage intention. |
| 2. | H2 | Perceived confidentiality has a positive relationship with e-banking usage intention. |
| 3. | H3 | Perceived data integrity has a positive relationship with e-banking usage intention. |
| 4. | H4 | Perceived non-repudiation has a positive relationship with e-banking usage intention. |

# CHAPTER 3

# RESEARCH METHODOLOGY

## 3.1 Introduction

In this part, the model of Chapter 2 is conveyed advance and get ready for testing. In accordance with the research questions and objectives, just as previous literature review, different methodologies are utilized to test the propose research model whether it concurs with the theories and the procedure receive for the assortment of information. This part contains nine sections, starting with the introduction followed by the research design in the second section. The third section examines the population and sampling size.

This is followed by the fourth section which clarify data collection procedure and the questionnaire design in the fifth section. The questionnaire development just as the unwavering reliability and validity of the instruments use in this investigation and measurement of variables and construct are remember for the sixth and seventh section individually. Section eight is give exclusively on plan of data analysis. At last, section nine gives the rundown of this section which is summary of the chapter. A questionnaire is lead to assemble the essential information for this quantitative research.

### 3.2 Research Design

The research design of this study is to decide if there is connection between at least two variables. In particular, this study will research the connection between security towards customers intention in Internet banking. The huge impacts of safety measurements on customers' intention to keep utilizing Internet banking are additionally being analyze. The reason for this study is to distinguish the security factors that impact intention to keep utilizing Internet banking in Malaysia. Information is gather using quantitative method distribute through the questionnaire to all individuals who use internet banking, which then they answer the questionnaires using a google form. The respondents participating in the survey must be include are Internet banking customers in Malaysia.

Information comes from individual Internet banking customers who perform banking exchanges by means of Internet banking. This is a descriptive research with an overview technique. The primary data is gather utilizing the quantitative technique to test the hypotheses. The data is collect using multiple choice questionnaires that are flow to respondents utilizing the questionnaire technique. Questionnaire are valuable to gather sections information, genuine belief, realities, or perspectives from respondents. Uniform plan and normalization are two of the main attributes of a study structure. The unit of analysis in a study are individuals. The questionnaires are disseminated by means of online such as media social where this question is given to individuals who use internet banking in Malaysia.

### 3.3 Population and Sample Size

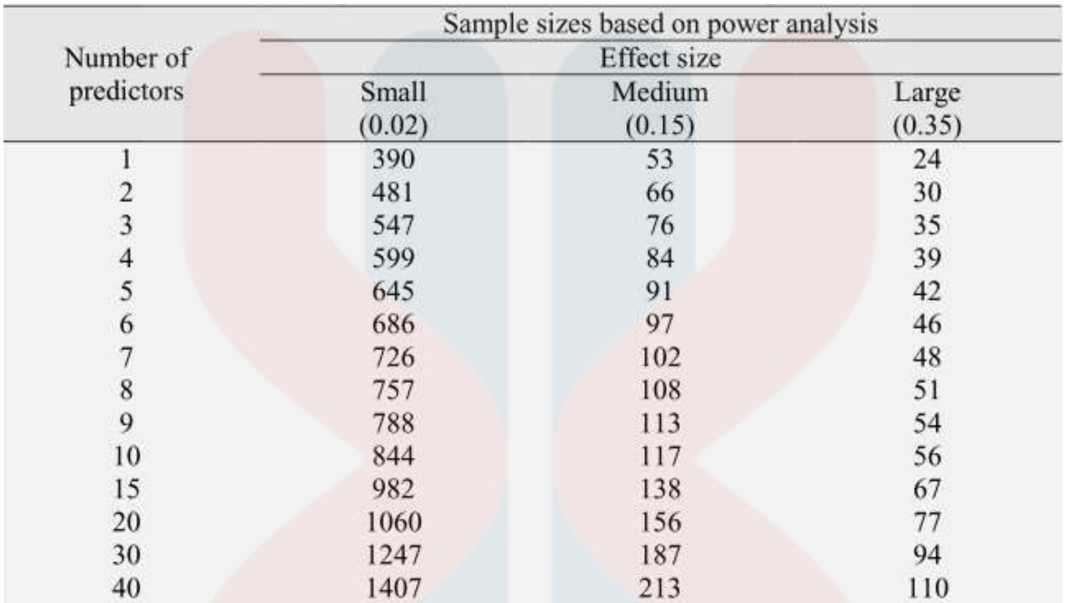
A population as a collection of people who share at least one attribute that sets them apart from other people (Kahn et al., 2006). Individuals who have use E-banking on a frequent basis in

Malaysia make up the study's sample. Individuals are the unit of analysis in this research. The E-banking users that have a desire for banking services in all of Malaysia represents in this study report. As of March 2021, Malaysia's population of persons who may be more incline to utilize E-Financial and then have a desire for banking services is 37.6 million (Bank Negara Malaysia, 2021).

A sample is a smaller version that may be use by a larger audience. It's a subset that includes a larger percentage of the population. When some other overall population grows too large for the sampling to contain those individuals or supervisors that are achievable, samples are utilize in data analysis. A sample must represent the entire population and not indicate any preference for one attribute over another. The researcher will actually want to draw discoveries that are generalizable to the target group after doing study on the sample. In accordance with the research purpose, individuals who have use E-banking on a frequent basis in Malaysia make up the study's sample, aged from 18 to 50, were chosen as the targeted sample since this cluster of people are more likely to use E-Banking and have a demand for banking services.

Table 3.1 illustrates the sample size need to test the hypothesis that multiple population correlations are equal to zero with a power of 0.8 (Alpha =.05) as recommend by Green et al. (1991). The minimal sample size may be determine using the greatest number of paths leading toward a single construct. By referring table below, the sample size suggested four predictors is 84 and effect size ($f^2$) of 0.15. A sample size of 150 respondents is suitable for this study to achieve a power of 80% and a significance level of 0.05 percent.

Table 3. 1: Sample Size Required to Test the Hypothesis that the Population Multiple Correlation Equals Zero with a Power of .80 (Alpha = .05)



| Number of predictors | Sample sizes based on power analysis | | |
|---|---|---|---|
| | Effect size | | |
| | Small<br>(0.02) | Medium<br>(0.15) | Large<br>(0.35) |
| 1 | 390 | 53 | 24 |
| 2 | 481 | 66 | 30 |
| 3 | 547 | 76 | 35 |
| 4 | 599 | 84 | 39 |
| 5 | 645 | 91 | 42 |
| 6 | 686 | 97 | 46 |
| 7 | 726 | 102 | 48 |
| 8 | 757 | 108 | 51 |
| 9 | 788 | 113 | 54 |
| 10 | 844 | 117 | 56 |
| 15 | 982 | 138 | 67 |
| 20 | 1060 | 156 | 77 |
| 30 | 1247 | 187 | 94 |
| 40 | 1407 | 213 | 110 |

### 3.3.1 Sampling Technique

According to Yin et al. (2003), the individual is frequently use as the unit of analysis in any study concerning individuals since researchers examine people. This study employs non-probability sampling techniques. Purposive Sampling strategies are chosen for this non-probabilistic sampling method. The sampling here is confined to specific types of individuals who can provide the desired information, because they have use E-banking on a frequent basis in Malaysia. Subjects are conveniently chosen from targeted groups according predetermined number or quota. However, since this is a non-probability sampling plan, the results are not generalizable to the population.

### 3.4 Data Collection Procedure

The procedure to gather the information is talked about in this part. As state beforehand, the information is gathered by utilizing study questionnaire that are circle to respondents utilizing the online survey. The questionnaire comprises of six sections. The primary area gathers the demographic information, the second till sixth sections inspire data about security factors and intention to keep utilizing Internet banking in Malaysia. The research technique use in this study is purposive sampling in light of the fact that this strategy is keep to explicit sorts of individuals who can give the longing data which are Internet banking customer. The survey questionnaire will be distributed to selected respondents who use internet banking in Malaysia through social media such as WhatsApp, Facebook and many more.

### 3.5 Questionnaire Design

Hypothesis testing fills in as the reason for this observational study. Forecasts are made by alluding to past writing and to legitimize the connection between both exogenous and endogenous factors. Inductions are drawn from the gather information utilizing a quantitative investigation. The questionnaire is configuration to quantify the effect of security factors that influences the intention towards E-banking use. Consequently, the reason for the questionnaire is to decide the respondents' discernments on the estimation things that are foreordain, structure, and characterize. Be that as it may, the study is a self-revealing questionnaire where the respondents are not guide and are separated from everyone else while addressing the inquiries.

As per Oppenheim et al. (1992), the methods of the questionnaire are a regularly use study procedure in sociology research, empowering information assortment in a design route for structure study. The principle work of a questionnaire is to measure the opinion and statement of respondents. There is only one form of a questionnaire for this study which is in the form of the online survey form. The “google form” online survey will be utilized. Therefore, the following sections are identified and categorize to form the basic structure of the questionnaire. There are six areas in the questionnaire where it contains clear and basic guidelines for each sections. Around, it requires around 10-15 minutes to finish the survey. Things for the survey are drawn from past investigations. These inquiries are on a five-point Likert scale from strongly disagree to strongly agree.

Section A is related to respondents’ profile (demographics and organizations). This section contains 10 questions, covering the respondent gender, age, race, highest academic qualification, occupation, working experience (total number of years), total number of years of internet usage, total number of years of internet banking usage and primary place of Internet banking use.

Section B consists of questions about the dependent variable which is behavioral intention. There are 5 questions about the construct of behavioral intention. In this sections, the study plans to gauge how much the respondents feel about their expectation in using E-banking for the previous years.

Section C consists of questions about the first independent variable. There are 4 questions about the construct of perceived authentication. In this section, respondents are required to rate their view e-banking protection in terms of perceived security concerns, safe transactions, and adequate mechanisms.

Section D comprise of inquiries regarding the second autonomous variable; perceived confidentiality. There are 4 identify with apparent secrecy. This section measures the effect of a confidentiality toward their E-banking utilization which identify with the more extensive idea of data security: restricting admittance to people's very own data. Respondents are need to guarantee that data is share just among approve people or associations.

Section E consist of questions about the third independent variable; perceived data integrity. There are 4 question relate to perceived data integrity. In this sections, the investigation plans to quantify how much the respondent dependability of data assets in them guaranteeing that data is adequately precise for its motivations.

Section F consists of questions about the fourth independent variable. There are 4 questions about the construct of perceived non-repudiation. In this section, respondents require to rate their view e-banking protection in terms of perceived non-repudiation whether their concerns of the authenticity of their signature on a document or the sending of a message.

## 3.6 Questionnaire Development

As indicated by Collis et al. (2003), survey are considered to be appropriate information assortment strategies in overviews that include a generally enormous example. The inquiries in the questionnaire ought to be basic and justifiable (Kumar et al., 2014). Besides, the format of the survey should make it simple and wonderful to peruse, the arrangement of inquiries ought to work with respondents while reacting and the things ought to be exact (Babbie et al., 2014; Kumar et al., 2013; Kumar et al., 2014). Otherwise, Krosnick et al. (2010) additionally stress that the survey should utilize basic and recognizable words as opposed to utilizing specialized terms, language or slang.

Likewise, long, multifaceted nuance questions and inquiries with single or twofold refutations that could delude respondents ought to likewise be stay away from. Questionnaires are utilized to gather data in comparative investigations rundown (Suh et al., 2002; Lee et al., 2001; Chellappa et al., 2002). The inquiries are classified as per the security target they allude to, hence keeping the members from getting befuddle, missing inquiries and other such issues (Dillman et al., 2000). To gauge the view of safety and social aim the things create in the survey are to be adjust from past investigations including (Suh et al., 2003; Yousafzai et al., 2005). The survey and things are then altered dependent on the input from a pilot study group. The survey comprises of close inquiries and no close to personal inquiries would be incorporate. The responses for the inquiry set are address by the Likert scale, permitting to respondents to choose the degree of effect the destinations allude to had on their trust (Collis et al., 2003). This empower scoring the answers and measurement of the study discoveries (Dawis et al., 1987). The Likert Scale is additionally like in the investigations survey. The questionnaire is making out of five fundamental sections for view of security and conduct intention separately.

### 3.6.1 Validity of the Instrument

The degree to which an action is without inclination (blunder free) means that the unwavering quality of the action and along these lines' reliable estimation across time and across the different things in the instrument is guarantee. The soundness and consistency with which the instrument estimates the idea and assists with surveying the "integrity" of an action show unwavering quality of an action (Sekaran et al., 2006). Reliability coefficient evaluates the consistency of the whole scale with Cronbach Alpha being the most generally use measure (Nunnally et al., 1979). Then again, the legitimacy is the degree to which an instrument estimates what it should quantify (Wiersma et al., 2000).

At this stage, the contribution of the supervisor as a guide is critical. Prior to continuing to academic scholar review, supervisor has been designated as editor to edit and survey the questionnaire for both English language and Malay language. This drive is to acquire criticism on the review instrument with respect to the design and language use just as ideas for development to guarantee that respondents can without much of a stretch comprehend the questionnaire and finishes it. This methodology is likewise central as any blunders and imperfections in the survey's plan can be relate to criticism from specialists. Surveys need to seem propelling and engaging for respondent to expand the reaction rate. Other than that, this cycle is useful in approving the succinctness and consistency of the Malay rendition of the survey. A duplicate of the survey is given to analysts. The analysts are needed to finish the survey and "verbally process" while doing that. Along these lines, the investigation can decide whether commentators comprehend the inquiries. They are then inquiry concerning mistakes in the survey and are request to remark or make ideas relating the inquiry length, design, and configuration just as the quantity of lines for answers, the inquiry arrangements and different issues.

### 3.6.2 Pilot Study

The possibility of a pilot study is to assess the unwavering quality and legitimacy of inquiries prior to leading the investigation (Vaus et al., 2002). A pilot study is made by overseeing the inquiries to a comparative, however more modest example to that which is to be use in the real investigation and it will show how a variable, as characterize for our motivations, can best be measure in the field (Siraj et al., 2012). A pilot study is a limited scale preliminary before the fundamental study, plan to survey the sufficiency of the exploration plan and the instruments to be use for information assortment; guiding the information assortment instruments is fundamental, regardless of whether meeting timetables or survey are use (Sapsford et al., 2006). The reliability and validity problems may emerge because of the presence of ambiguities in the inquiries plan. Pretesting the survey before genuine administration can limit the presence of ambiguities plausibility.

The actions looked over past study on conduct intention and security in the E-banking industry could then be modify and adjust as indicated by the objectives of this exploration. A pilot study is lead to get input on the survey plan and simplicity of understanding the inquiries. For the pilot test, 30 questionnaires are conveyed haphazardly to Malaysian guaranteeing the adequacy of the survey. As per DeMaio et al. (2004), pretesting of the instrument is a significant advance on the grounds that the consequence of the pre-testing will demonstrate whether the overview is effective in gathering the aims of the investigation. Tatham et al. (1998) declare that proportions of dependability that reaches from 0 to 1, with upsides of .60 to .70 consider the lower furthest reaches of agreeableness. Nunnally et al. (1979) suggest >.70 as the worthiness level. In view of this input the survey is then to be reexamine before the last study. To ensure the clarity and suitability of the questions, a pilot survey with a sample of 30 Malaysians is distributed indiscriminately. The privacy and confidentiality of the replies were guaranteed to responders in order to secure a valid and most accurate answer. The respondents were not obliged to provide their names or addresses, which may have revealed their identities. The pilot study was also important for identifying survey instrument problems. Question wording, sequencing, layout, respondent familiarity, questionnaire completion time, and analytic procedure can all be used to identify them.

In the pilot research, the factors of intention to utilise e-banking revealed that there was some misunderstanding among the respondents. The intention to use e-banking for the pilot test had a reliability of 0.469. By checking all of the assertions, the researcher enhances the reliability values and found out that third question “If I could, I would like to discontinue my use of Internet banking services” was a negative statement and the action take by the researches was delete the statements from the questionnaires. And the new Cronbach’s Alpha was 0.828. The other variables (Perceived authentication, Perceived confidentiality, Perceived data integrity and Perceived non-repudiation) showed an adequate reliability with Cronbach’s alpha values, which ranged from 0.744 to 0.891 that are considered acceptable reliabilities. Therefore, the construct measures are considered reliable.

Table 3.2: Reliability Coefficient for the Variables in Pilot Study

| Variables | Alpha |
|---|---|
| Intention to Use E-Banking | 0.828 |
| Perceived authentication | 0.844 |
| Perceived confidentiality | 0.744 |
| Perceived data integrity | 0.890 |
| Perceived non-repudiation | 0.891 |

## 3.7 Measurement of Variables and Construct

The estimation model guides the actions into a hypothetical build where exogenous factors and endogenous factors are separate. The exogenous develop is frequently known as the free factor which is the indicator that clarifies the difference in the endogenous variable (subordinate variable). In this study, the exogenous factors are the security factors incorporate the Perceived authentication, Perceived confidentiality, Perceived data integrity and Perceived non-repudiation. The endogenous variable, otherwise called the ward or measure variable is the center of this study, where different factors in the model depict it.

In this study, the intention got is the endogenous variable. Sets of instruments that are approve which are address as markers or things are used to gauge the factors. The accompanying area examine the estimation and operationalize idea of the factors.

### 3.7.1 Measurement of Variables

This section presents the measurement items use in this study. The dependent variable in this study is behavioral intention. The independent variables in this study Perceived authentication, Perceived confidentiality, Perceived data integrity and Perceived non-repudiation.

Table 3.3: Measurement of Variables

| Variables | Sources | No. of Items |
|---|---|---|
| Intention to Use E-Banking | (Bhattacherjee et al., 2001; Chung et al., 2007) | 5 |
| Perceived authentication | (Suh et al., 2003) | 4 |
| Perceived confidentiality | (Suh et al., 2003) | 4 |
| Perceived data integrity | (Suh et al., 2003) | 4 |
| Perceived non-repudiation | (Suh et al., 2003) | 4 |
| **Total** | | **21** |

### 3.7.2 Operationalization of Variables

An ordinal scale is utilized in this investigation which incorporates a Likert scale in the survey. This is because of the abstract idea of factors where they can't be measure genuinely. The scale comprises of a fix decision question design which address singular mentality, trust, assessment, and feeling in the estimation of factors. Respondents are need to show their degree of understanding, fulfillment, or different reactions for the assertions in the survey which range from the most reduced level to the most significant level. Every reaction is given a point esteem where the absolute worth would decide the respondent's score (Croasmun et al., 2011).

There are several types of questions in these sections such as multiple choices with only one answer, multiple choice with only multiple answers, ranking, and matrix choices with five (5) points Likert scales. For section ‘B’ to section ‘F’, respondents will be asking to indicate the degree of their agreement with each statement by circling only one of the five alternatives score. The statement will be measure by using Likert Scale five (5) points. The range is from strongly disagree (1) to strongly agree (5) as suggest by (Wong et al., 2013). According to Oppenheim et al. (1992), the Likert scale is the most appropriate procedure to measure attitude. Subsequently, the information can be utilized to accomplish more noteworthy factual dynamic and certainty.

### 3.7.3 Research Instrument Development

This part presents the estimation things use in this investigation. The reliant variable in this study is intention. The autonomous factors in this study perceived authentication, perceived confidentiality, perceived data integrity and perceived non-repudiation.

#### 3.7.3(a) Intention to use E-banking

Behavioral intention alludes to an individual's ability to participate in a given conduct. This variable is measure utilizing 6 things adjust from Bhattacherjee et al. (2001) and Chung et al. (2007) in which respondents rate the degree of concur as far as the conduct expectation in E-banking utilization. They are given a choice of five values by using Likert Scale five (5) points. The range is from strongly disagree (1) to strongly agree (5) as suggest by (Wong et al., 2013).

Table 3.4 presents the items for the performance of intention to use E-banking.

| Items |
|---|
| 1. I intend to continue using Internet banking services rather than discontinue its use. |
| 2. My intentions are to continue using Internet banking services than use any alternative means (traditional banking). |

| |
|---|
| 3. If I could, I would like to discontinue my use of Internet banking services. |
| 4. I intend to continue using Internet banking services whenever I need it. |
| 5. I intend to continue using Internet banking service feature since it is good. |

### 3.7.3(b) Perceived Authentication

Authentication refers to a method in which users must affirm their identities by completing a validation process. This variable is measure utilizing 4 things adjust from Suh et al. (2003) in which respondents rate the degree of concur as far as the verification in E-banking. They are given a decision of five qualities by utilizing Likert Scale five (5) points. The range is from strongly disagree (1) to strongly agree (5) as suggest by (Wong et al., 2013).

Table 3.5 presents the items for the performance of perceived authentication

| Items |
|---|
| 1. The transactions I send are transmitted to my Internet banking site. |
| 2. The messages I receive are transmitted from my Internet banking site. |
| 3. My Internet banking site ascertains my identity before sending any messages to me. |
| 4. My Internet banking site ascertains my identity before processing the transaction received from me. |

### 3.7.3(c) Perceived confidentiality

Confidentiality is vital in the internet business world in view of the likelihood that programmers may acquire one's touchy data. This variable is measure using 4 items adapt from Suh et al. (2003) in which respondents rate the level of agree in terms of the confidentiality in E-banking. They are given a choice of five values by using Likert Scale five (5) points. The range is from strongly disagree (1) to strongly agree (5) as suggest by (Wong et al., 2013).

Table 3.6 presents the items for the performance of perceived confidentiality

| Items |
|---|
| 1. All the communication with my Internet banking site is strictly within the site and me. |
| 2. I am convinced that my Internet banking site respects the confidentiality of the transactions received from me. |
| 3. My Internet banking site uses some security controls for the confidentiality of the transactions. |
| 4. My Internet banking site checks all communications between the site and me for the protection from wiretapping or eavesdropping. |

### 3.7.3(d) Perceived data integrity

Data integrity implies that information in transmissions are not make, catch, change or erase unlawfully. This variable is measure using 4 items adapted from Suh et al. (2003) in which respondents rate the level of agree in terms of the data integrity in E-banking. They are given a choice of five values by using Likert Scale five (5) points. The range is from strongly disagree (1) to strongly agree (5) as suggest by (Wong et al., 2013).

Table 3.7 presents the items for the performance of perceived data integrity

| Items |
|---|
| 1. My Internet banking site checks the information communicated with me for accuracy. |
| 2. My Internet banking site takes steps to make sure that the information in transit is accurate. |
| 3. My Internet banking site takes steps to make sure that the information in transit is not deleted. |
| 4. My Internet banking site devotes time and effort to verify the accuracy of the information in transit. |

**3.7.3(e) Perceived non-repudiation**

Non-repudiation is an instrument to guarantee that the customers can be sure they are speaking with the authentic worker (bank), or the other way around. This variable is measure using 4 items adapt from Suh et al. (2003) in which respondents rate the level of agree in terms of the non-repudiation in E-banking. They are given a choice of five values by using Likert Scale five (5) points. The range is from strongly disagree (1) to strongly agree (5) as suggest by (Wong et al., 2013).

Table 3.8 presents the items for the performance of perceived non-repudiation

| Items |
|---|
| 1. My Internet banking site will not deny having participated in a transaction after processing it. |
| 2. My Internet banking site will not deny having received a transaction from me. |

| |
|---|
| 3. My Internet banking site will not deny having sent me a message. |
| 4. My Internet banking site provides me with some evidence to protect against its denial of having received a transaction from me. |

## 3.8 Data Analysis

### 3.8.1 Data analysis using SPSS

Statistical Package for the Social Sciences (SPSS) will be use to generate and evaluate the data obtain (SPSS). There will be two steps to the data analysis. First before descriptive statistics techniques are employ to evaluate the data, the first phase of the analysis is doing a descriptive statistical analysis to explore the data. Mean values, average scores, and comparative scores with each of the scales will be determine for each response. The following study will be based on these facts. Overall means, standard deviation, and skewness among data (person involve scores) for each factor will be compute, along with accurate system operations. After that, the data will be converted. Cronbach alphas will be use to check for content validity.

### 3.8.2 Descriptive Statistics

In the second step, several statistical approaches are used to evaluate the study questions. Descriptive statistics are used to evaluate the contributions each of the determinants of security on E-banking usage intention to the variation and to manage some variables while evaluating for statistically impacts of the others. Throughout this study, descriptive statistics are performed to examine demographics data collect from the survey, such as gender, academic background, working tenure, and position, all of which are verify by the descriptive statistical analysis. The statistical method will begin by manipulating the data in the following phases. Raw scores, average scores, and relative scores will be generated for each response on each of the scale. The future evaluation will be based on this information.

### 3.8.3 Reliability Analysis

Reliability analysis were used in this study to determine the acceptance and validity of the questionnaire. Therefore, the survey questionnaire will be distributed to selected respondents who use internet banking in Malaysia. Cronbach's Alpha was used to determine whether the study was reliable or not. Cronbach Alpha which is one of the reliability tests conducted in SPSS. There are basically two alpha versions in the reliability analysis, namely the normal and standard versions. The normal version was used to measure the variables of this study for which the alpha normal version is typically used when items are scaled to produce a single score for that scale. The acceptable reliability value is .6. When the reliability result of the questionnaire is above 6 then your questionnaire is considered "reliable". In addition, the question was on a 5 -point Likert Scale with answers ranging from "Strongly agree" to "Strongly disagree". To determine whether the questionnaire can be "reliable" measure the variables. Thus, it is evident that Cronbach's Alpha has been able to measure the variables of interest accurately in this study. The statistics is considered applicable for further analysis.

### 3.8.4 Correlation Analysis

This study contains four independent variables. The variables are perceived authentication, perceived confidentiality, perceived data integrity and perceived non-repudiation. Correlation analysis is to determine how independent variables interrelate with dependent variables which intention to use E-banking.

## 3.9 Conclusion

To conclude, this chapter discuss the quantitative analytical approach that will be use in this study. To confirm this model, a review procedure is found to appropriate. A primer advance in this study is to distinguish estimation things for security and trust from earlier writing and confirm these through a pilot study. This is then followed by the assortment of information through a survey. An arbitrary example of understudies is chosen for the investigation. While this example is a little subset of the E-banking customer population, the variety on the grounds guarantees that this example is illustrative of the population. The steps to be undertaken by the researcher begins with the aims of the research, the identification of the sample, the instruments (questionnaire) to be use and the mode of data analysis.

# CHAPTER 4

# DATA ANALYSIS AND FINDINGS

## 4.1 Introduction

This chapter, which is divided into eight sections, covers data analysis and gives empirical findings that support the study hypotheses. The first section is an introduction, while the second and third sections present a preliminary analysis that includes data screening, missing data, and straight lining, as well as the demographic profile of respondents. The following part discusses descriptive analysis. Section five reports the results of the measurement items used it to analyse the structures' reliability and validity, followed by section six, which explains data normality. Section seven contains the results of hypothesis testing. The eighth section concludes with a brief summary of this chapter.

## 4.2 Preliminary Analysis

### 4.2.1 Data Screening

Data were checked for data entry accuracy, missing values, and violation of multivariate statistical assumptions using SPSS version 25 before to the multivariate analysis. However, there is no missing data and straight lining data in our respondents, therefore all data are usable. All respondents were fitted with our respondent's criteria which are the age of respondents 18 – 50 years only. There are 153 respondents that are available and valid for the analysis.

### 4.2.2 Missing Data

Missing data is frequently problematic since several research projects have used survey technique to acquire data. Missing data happens when a respondent, whether deliberately or unconsciously, fails to finish the questionnaire or respond to one or more questions. If an initial threshold of more than 15% for missing data is achieved, it is prudent to exclude data observation (Hair, Hult, Ringle, & Sarstedt, 2017). None of the study variables had many missed subjects (more than 15 per cent). As a result, we used all the components in the analysis. For the next screening phase, however, all 153 questionnaires were kept in liner terminology, further explained in section 4.2.3.

### 4.2.3 Straight Lining

An additional data filtering technique that was applied was an uncertain reaction pattern. Forms are properly checked for a problematic approach, such as straight-lining, as a result of this change. When a respondent marks the same response for the collective topics, this is referred to as a straight-lining design. According to Hair et al., (2017), any questionnaire responses having a suspicious reply, such as straight-lining, will be deleted.

We determined that all 153 surveys were legitimate and did not include any questionable elements. The specific response on the 5-point Likert scale for each detail is associated. As a result, 153 surveys were discovered to be correctly coded and analysed.

## 4.3 Demographic Profile of Respondents

The general background of those who answered the questionnaire in this study was the second piece of information that was looked at. To make things easier to understand, all data is provided in actual numbers and percentages. A total of 153 people answered the survey. This section of the inquiry is made up of data on age, gender, race, level of education, status of employment, income, usage of internet, usage of E-banking, and places of primary as shown in the Table 4.1 below.

Table 4.1: Profile of Respondents

| Background | Information | Frequency | Percentage (%) |
|---|---|---|---|
| **Age** | < 20 years | 5 | 3.3 |
| | 20-29 years | 143 | 93.5 |
| | 30-39 years | 4 | 2.6 |
| | 40-49 years | 1 | 0.7 |
| | | | |
| **Gender** | Male | 38 | 24.8 |
| | Female | 115 | 75.2 |
| | | | |
| **Race** | Malay | 147 | 96.1 |
| | Chinese | 3 | 2.0 |
| | Indian | 1 | 0.7 |
| | Others | 2 | 1.3 |

|  |  |  |  |
|---|---|---|---|
|  |  |  |  |
| **Education Level** | SPM | 12 | 7.8 |
|  | STPM | 14 | 9.2 |
|  | Certificate | 3 | 2.0 |
|  | Diploma | 32 | 20.9 |
|  | Degree or higher | 92 | 60.1 |
|  |  |  |  |
| **Employment Status** | Student | 95 | 62.1 |
|  | Self-Employed | 10 | 6.5 |
|  | Private Sector | 26 | 17.0 |
|  | Government Sector | 7 | 4.6 |
|  | Others | 15 | 9.8 |
|  |  |  |  |
| **Income** | <RM2500 | 133 | 86.9 |
|  | RM 2501 – RM4850 | 16 | 10.5 |
|  | RM4851 – RM 10 970 | 4 | 2.6 |
|  |  |  |  |
| **Total years of Internet Usage** | <3 years | 3 | 2.0 |
|  | 3-6 years | 30 | 19.6 |
|  | 7-11 years | 64 | 41.8 |
|  | 12-15 years | 27 | 17.6 |
|  | >16 years | 29 | 19.0 |

|  |  |  |  |
|---|---|---|---|
|  |  |  |  |
| **Total years of E-Banking Usage** | <1 year | 17 | 11.1 |
|  | 1-10 years | 126 | 82.4 |
|  | 11-20 years | 8 | 5.2 |
|  | >20 years | 2 | 1.3 |
|  |  |  |  |
| **Primary Places of E-Banking Use** | Home | 131 | 85.6 |
|  | Office | 21 | 13.7 |
|  | Internet Cafe | 1 | 0.7 |

Table 4.1 shows the demographics of the 153 of Malaysian Internet banking customers. Age, gender, race, education level, work status, income, total number of years of internet usage, total number of years of online banking usage, and principal site of Internet banking usage are among the characteristics included in the data. The bulk of those who responded were young people, with about 93.5 % being between the ages of 20 and 29. The remainder age less than 20 years (3.3%), 30 - 39 years (2.6%), and 40 - 49 years (0.7%). More than half of the respondents were females (75.2%) and the remaining (24.8%) were males. Out of 153 respondents, only 1 (0.7%) comprised of Indians followed by Chinese which is 3 (2%). the majority of respondents are Malays which is 147 respondents (96.1%) followed. Meanwhile, the others, indigenous Sabahans and Sarawakians is 2 (1.3%). The respondents in this research generally covered all the states in Malaysia.

As for level of education, majority of the respondents have a Bachelor's degree and higher (60.1%). Majority of respondents were student (62.1%), while the remainder were self-employed

(6.5%), private sector (17.0%), government sector (4.6%) and others (9.8%). In terms of income background, 86.9% of the respondents have an income of less than RM2500, 10.5% earn between RM2501 – RM 4850 while the remaining 2.6% respondents make over RM4851 to RM 10970.

When it comes to internet usage, the majority of those polled had 7 to 11 years of experience (41.8%) in usage of internet. The remainder were less than 3 years (2.0%), 3 - 6 years (19.6%), 12 - 15 years (17.6%) and more than 16 years (19.0%). Majority of respondents have less than 10 years (82.4%) experience of usage E-banking. Last but not least, the majority of the respondent's places of primary were home (85.6%).

## 4.4 Descriptive Analysis

The mean, standard deviation, and variance for each variable were calculated in this part to fully explain the diversity and interrelation of the variables, which illustrate how respondents reacted to the questionnaire. As a result, descriptive statistics were utilised to define and highlight the key aspects of the data set from the respondents' viewpoints on all dimensions of behavioural intention, perceived authentication, perceived confidentiality, perceived data integrity, and perceived non-repudiation.

Table 4.2: Mean and Standard Deviation

| **Latent Variable** | **Items** | **Mean** | **Std. Deviation** |
|---|---|---|---|
| **Behavioral Intention** | B1 | 4.5490 | 0.67805 |
| | B2 | 4.3203 | 0.77505 |
| | B3 | 4.5556 | 0.59481 |
| | B4 | 4.4510 | 0.71581 |

| | | | |
|---|---|---|---|
| **Perceived Authentication** | C1 | 4.3529 | 0.73869 |
| | C2 | 4.2876 | 0.72251 |
| | C3 | 4.4248 | 0.68530 |
| | C4 | 4.4967 | 0.67982 |
| **Perceived Confidentiality** | D1 | 4.2614 | 0.77605 |
| | D2 | 4.3464 | 0.74622 |
| | D3 | 4.3529 | 0.69273 |
| | D4 | 4.2157 | 0.78591 |
| **Perceived Data Integrity** | E1 | 4.3660 | 0.70479 |
| | E2 | 4.4248 | 0.67564 |
| | E3 | 4.2353 | 0.74131 |
| | E4 | 4.3333 | 0.75219 |
| **Perceived Non Repudiation** | F1 | 4.1307 | 0.82472 |
| | F2 | 4.2026 | 0.82206 |
| | F3 | 4.2026 | 0.80590 |
| | F4 | 4.2941 | 0.75116 |

The mean value for all the constructs' variables from of the questionnaire form is shown in Table 4.2. A 5-point Likert-scale was used in the study, with values ranging from 1 to 5. The dependent variables (Behavioral Intention) are connected to the first six constructs in Table 4.2, followed by independent factors (perceived authentication, perceived confidentiality, perceived data integrity and perceived non repudiation). The dependent variable B3 had the highest mean score of 4.5556 (SD=0.59481). Other indicators had a mean that ranged from 4.3203 to 4.5556.

Perceived authentication (Mean=4.4967, SD=0.67982) and perceived data integrity (Mean=4.4248, SD=0.67564) were the two indicators with the highest values for independent variables. The perceived confidentiality indicator (Mean=4.3529, SD=0.69273) received the third highest score. Other independent variable indicators have a range of 4.1307 to 4.4967 as their mean. The perceived non repudiation indicator (Mean=4.1307, SD=0.82472) had the least value.

In sum, the mean value for each construct reveals that perceived authentication (Mean=4.3905, SD=0.56693) is the most important contributing factor for the performance of intention to use E-banking, followed by perceived data integrity (Mean=4.3399, SD=0.60739), as shown in Table 4.3. With a mean score of 4.2075 (SD=0.69585), perceived non-repudiation was the lowest component.

Table 4.3: Descriptive Statistics for Each Construct

| **Latent Variable** | **N** | **Minimum** | **Maximum** | **Mean** | **Std. Deviation** |
|---|---|---|---|---|---|
| **Behavioral Intention** | 153 | 3.00 | 5.00 | 4.4690 | 0.58018 |
| **Perceived Authentication** | 153 | 2.75 | 5.00 | 4.3905 | 0.56693 |
| **Perceived Confidentiality** | 153 | 2.75 | 5.00 | 4.2941 | 0.60909 |
| **Perceived Data Integrity** | 153 | 3.00 | 5.00 | 4.3399 | 0.60739 |
| **Perceived Non Repudiation** | 153 | 2.00 | 5.00 | 4.2075 | 0.69585 |

## 4.5 Validity and Reliability Analysis

The more reliable a set of scales or scale items is, the more sure we can be that the score gained from the researcher's test is essentially the same as the score acquired if the test were repeated. The question of if each scale is assessing a single thought is raised by reliability. It is a metric for determining the internal consistency of a set of scale items in a test. The purpose of a reliability test on methods used to assess construct is to ensure that the instruments used to measure the ideas are consistent. Validity testing, on the other hand, examines the extent to which the instruments designed measure the idea they are meant to assess (Hair, Ringle, et al., 2011).

The content validity was determined using a questionnaire that had already been completed by another researcher and published in the journal. In addition, a comprehensive literature search was conducted to improve content validity. Corrections and notes were made on the observations that had been made. Cronbach's Alpha was used to determine the instrument's reliability. As each construct's Cronbach's Alpha value reaches 0.7, a measurement model's internal consistency dependability is excellent; nevertheless, values of 0.8 or 0.9 are preferable in subsequent phases (Nunnally & Bernstein, 1979).

Table 4.4: Result of Cronbach’s Alpha

| Cronbach's Alpha | Cronbach's Alpha Basedon Standardized Items | N of Items |
|---|---|---|
| .947 | .947 | 20 |

Based on table 4.4, all the variables are analysed for reliability is 0.947 represent Cronbach's alpha coefficient. As a result, the questionnaire is reliable and appropriate for use in the research.

Table 4.5: Results of the Reliability Analysis on Constructs

| **Study Instruments** | **N of Items** | **Cronbach's Alpha** |
|---|---|---|
| **Behavioral Intention** | 4 | 0.856 |
| **Perceived Authentication** | 4 | 0.815 |
| **Perceived Confidentiality** | 4 | 0.826 |
| **Perceived Data Integrity** | 4 | 0.866 |
| **Perceived Non Repudiation** | 4 | 0.891 |

According to table 4.5, all existing research variables have a precise Cronbach Alpha estimate of more than 0.7. The table above contains 20 items that were tested using a reliability test. As a result, behavioural intention, which is a required variable across four items, has a large coefficient alpha of 0.856. Through 15 independent variables, the significant coefficient alpha of Perceived Authentication is 0.815. Aside from that, the Perceived Confidentiality factor has an alpha of 0.826. The following component, Perceived Data Integrity, has a coefficient apha of 0.866. The last component, Perceived Non Repudiation, has an alpha of 0.891. Overall, the overall reliability test results vary from 0.815 to 0.891, which are regarded good reliabilities and an encouraging indicator for the study. Furthermore, all responses to the variables passed the reliability test. All five variables are found to have significantly high reliability consistency.

## 4.6 Normality Test

The normality tests aid in the graphical evaluation of normality. The Kolmogorov-Smirnov test for normalcy is based on the most radical differentiation between actual appropriation and projected cumulative-normal dispersion (Ghasemi & Saleh Zahediasl, 2012). This exam has been shown to be less remarkable than other tests in general. It is included as a consequence of its long-standing importance. Shapiro-Wilk W is often the most remarkable test. When a frequency variable is specified, the test is not performed. (Das, 2016) The tests mentioned above compare the scores as in experiment to a group of scores that are normally distributed and have the same mean and standard deviation (Ghasemi & Saleh Zahediasl, 2012).

Standardisation measures are used in statistics to assess if a data set is modelled for normal distribution. Several statistical functions need a distribution to be expected or almost every day. For at least two factors, tests for normality are significant. Second, non-linearity and interacting physical systems typically contribute to non-Gaussian distributions. It is also possible to better understand the originating mechanism of the processes by analysing the chosen variables' distribution.

Therefore, for this reason, the Kolmogorov-Smirnov and Shapiro-Wilk, Q-Q Plot and skewness tests were used to test the normality. The results show that the data is not normal since the significance value is less than 0.05 and the skewness value is less than -1 as shown in table 4.7. The normality test results' details can be at the table 4.6 below:

Table 4.6: Tests of Normality

| | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|
| | Statistic | df | Sig. | Statistic | df | Sig. |
| Behavioral Intention | .206 | 153 | .000 | .841 | 153 | .000 |
| Perceived Authentication | .186 | 153 | .000 | .875 | 153 | .000 |
| Perceived Confidentiality | .158 | 153 | .000 | .907 | 153 | .000 |
| Perceived Data Integrity | .175 | 153 | .000 | .884 | 153 | .000 |
| Perceived Non Repudiation | .147 | 153 | .000 | .897 | 153 | .000 |

Table 4.7: Descriptive

| | | | Statistic | Std. Error |
|---|---|---|---|---|
| Behavioral Intention | Mean | | 4.4690 | .04690 |
| | 95% Confidence Interval for Mean | Lower Bound | .3763 | |
| | | Upper Bound | .5616 | |
| | 5% Trimmed Mean | | 4.5181 | |
| | Median | | 4.5000 | |
| | Variance | | .337 | |
| | Std. Deviation | | .58018 | |
| | Minimum | | 3.00 | |
| | Maximum | | 5.00 | |
| | Range | | 2.00 | |
| | Interquartile Range | | 1.00 | |

| | | | | |
|---|---|---|---|---|
| | Skewness | | -.932 | .196 |
| | Kurtosis | | -.057 | .390 |
| Perceived Authentication | Mean | | 4.3905 | .04583 |
| | 95% Confidence Interval for Mean | Lower Bound | 4.3000 | |
| | | Upper Bound | 4.4811 | |
| | 5% Trimmed Mean | | 4.4309 | |
| | Median | | 4.5000 | |
| | Variance | | .321 | |
| | Std. Deviation | | .56693 | |
| | Minimum | | 2.75 | |
| | Maximum | | 5.00 | |
| | Range | | 2.25 | |
| | Interquartile Range | | 1.00 | |
| | Skewness | | -.593 | .196 |
| | Kurtosis | | -.359 | .390 |
| Perceived Confidentiality | Mean | | 4.2941 | .04924 |
| | 95% Confidence Interval for Mean | Lower Bound | 4.1968 | |
| | | Upper Bound | 4.3914 | |
| | 5% Trimmed Mean | | 4.3274 | |
| | Median | | 4.2500 | |
| | Variance | | .371 | |
| | Std. Deviation | | .60909 | |
| | Minimum | | 2.75 | |
| | Maximum | | 5.00 | |
| | Range | | 2.25 | |
| | Interquartile Range | | 1.00 | |
| | Skewness | | -.452 | .196 |
| | Kurtosis | | -.741 | .390 |
| | | | Statistic | Std. |

| | | | | Error |
|---|---|---|---|---|
| Perceived Data Integrity | Mean | | 4.3399 | 04910 |
| | 95% Confidence Interval for Mean | Lower Bound | 4.2429 | |
| | | Upper Bound | 4.4369 | |
| | 5% Trimmed Mean | | 4.3776 | |
| | Median | | 4.5000 | |
| | Variance | | 369 | |
| | Std. Deviation | | 60739 | |
| | Minimum | | 3.00 | |
| | Maximum | | 5.00 | |
| | Range | | 2.00 | |
| | Interquartile Range | | 1.00 | |
| | Skewness | | -.586 | 196 |
| | Kurtosis | | -.565 | 390 |
| Perceived Non Repudiation | Mean | | 4.2075 | 05626 |
| | 95% Confidence Interval for Mean | Lower Bound | 4.0964 | |
| | | Upper Bound | 4.3187 | |
| | 5% Trimmed Mean | | 4.2397 | |
| | Median | | 4.2500 | |
| | Variance | | 484 | |
| | Std. Deviation | | 69585 | |
| | Minimum | | 2.00 | |
| | Maximum | | 5.00 | |
| | Range | | 3.00 | |
| | Interquartile Range | | 1.25 | |
| | Skewness | | -.534 | .196 |
| | Kurtosis | | -.527 | .390 |

### 4.6.1 Correlation Analysis

The analysis of correlations (Hotelling, 1936; Anderson, 1984) is a common statistical approach for finding linear projections of two maximum correlated random vectors. Correlation analysis was utilised for unsupervised data processing when numerous viewpoints were available (Hardoon et al., 2007; Vinokourov et al., 2003; Dhillon et al., 2011). Correlation Analysis is a statistical method for determining whether or not two variables or data sets have a link and how strong that relationship is. That instance, in market research, correlation analysis is used to assess whether there were any noteworthy correlations, patterns, or trends between objective data acquired through research methodologies such as surveys. Spearman correlation was calculated based on the normality test result to analyse the link between security factors and the intention to continue using Internet banking.

## 4.7 Hypothesis Testing

### 4.7.1 Spearman's Correlations Analysis

Spearman's correlation coefficient is a test statistic that determines the statistical link between two continuous variables (independent and dependent variables). The purpose of this test is to see if the correlation coefficient is significant, as well as to figure out which hypotheses are accepted and thus should be rejected. Based on the table below, the significant value (p-value) is less than alpha (0.05), which means a significant relationship exists between independent and dependent variables.

Table 4.8: Spearman Correlation Coefficient Analysis

| | | | Mean Behavioral Intention | Mean Perceived Authentication |
|---|---|---|---|---|
| Spearman's rho | Mean Behavioral Intention | Correlation Coefficient | 1.000 | .735** |
| | | Sig. (1-Tailed) | . | .000 |
| | | N | 153 | 153 |
| | Mean Perceived Authentication | Correlation Coefficient | .735** | 1.000 |
| | | Sig. (1-Tailed) | .000 | . |
| | | N | 153 | 153 |

| | | | Mean Behavioral Intention | Mean Perceived Confidentiality |
|---|---|---|---|---|
| Spearman's rho | Mean Behavioral Intention | Correlation Coefficient | 1.000 | .633** |
| | | Sig. (1-Tailed) | . | .000 |
| | | N | 153 | 153 |
| | Mean Perceived Confidentiality | Correlation Coefficient | .633** | 1.000 |
| | | Sig. (1-Tailed) | .000 | . |
| | | N | 153 | 153 |

| | | | Mean Behavioral Intention | Mean Perceived Data Integrity |
|---|---|---|---|---|
| Spearman's rho | Mean Behavioral Intention | Correlation Coefficient | 1.000 | .632** |
| | | Sig. (1-Tailed) | . | .000 |
| | | N | 153 | 153 |
| | Mean Perceived Data Integrity | Correlation Coefficient | .632** | 1.000 |
| | | Sig. | .000 | . |

| | | | | |
|---|---|---|---|---|
| | | (1-Tailed)<br>N | 153 | 153 |
| | | | Mean Behavioral Intention | Mean Perceived Non Repudiation |
| Spearman's rho | Mean Behavioral Intention | Correlation Coefficient<br>Sig. (1-Tailed)<br>N | 1.000<br>.<br>153 | .525$^{**}$<br>.000<br>153 |
| | Mean Perceived Non Repudiation | Correlation Coefficient Sig. (1-Tailed)<br>N | .525$^{**}$<br>.000<br>153 | 1.000<br>.<br>153 |

Table 4.8 represents spearman Correlation coefficient analysis. This assessment is to validate the relationship of E-banking usage intention and perceived authentication. The result shows there is a positive relationship between E-banking usage intention and perceived authentication, r = 0.735, n = 153, p= 0.000.Therefore hypothesis one is accepted. There is positive and high relationship between E-banking usage intention and perceived confidentiality.

Next is second relationship of E-banking usage intention and perceived confidentiality. The result shows there is a positive relationship between E-banking usage intention and perceived confidentiality, r = 0.633 n = 153, p= 0.000. The analysis conclude that there is positive and high relationship between E-banking usage intention and perceived confidentiality.

Meanwhile, third is relationship of E-banking usage intention and perceived data integrity. The result shows there is a positive relationship between E-banking usage intention and perceived data integrity, r = 0.632, n = 153, p= 0.000. The analysis concludes that there is positive and high relationship between E-banking usage intention and perceived data integrity.

Lastly is relationship of E-Banking usage intention and perceived non-repudiation. The result shows there is a positive relationship between E-Banking usage intention and perceived non-repudiation, r = 0.525, n = 153, p= 0.000. The analysis concludes that there is positive and high relationship between E-Ban king usage intention and perceived non-repudiation.

### 4.7.2 Summary of Hypothesis

Table 4.9: Summary of Hypothesis

| Hypothesis | Relationship | Correlation | Result |
|---|---|---|---|
| H1 | There is a significant positive relationship between E-Banking usage intention and perceived Authentication | Moderate | Support |
| H2 | There is a significant positive relationship between E-Banking usage intention and perceived Confidentiality | Moderate | Support |
| H3 | There is a significant positive relationship between E-Banking usage intention and perceived Data Integrity | Moderate | Support |
| H4 | There is a significant positive relationship between E-Banking usage intention and perceived Non-repudiation | Moderate | Support |

## 4.8 Summary

This chapter included the data analysis for the research, including the backgrounds of the respondents, the results of the assessment measurement model, and the structural model built with SPSS IBM version 26. The research aims guided the development of the main topics. According to this study, the intention to use internet banking in Malaysia is connected to perception of authentication, confidentiality, data integrity, and non-repudiation. The intention to use online banking in Malaysia is linked to perceived authentication, confidentiality, data integrity, and non-repudiation, according to this study.  According to the survey, Malaysians' desire to use online banking is influenced by perceived authentication. It's because authentication is defined as the process of creating an online merchant through a trusted third party and ensuring that the merchant and the trade partners in an electronic transaction or communication are who they say they are.

Customers' identities are validated using a variety of methods and access codes, including unique usernames, personal identification numbers (PINs), passwords, and specified verification queries. These tools are used to get access to customers' personal accounts and financial information, as well as banking services, goods, and services offered through the online banking system. Customers are advised to keep their personal codes safe by not sharing or providing easy access to them. Non-repudiation, on the other hand, is considered as a minor factor in Malaysians' willingness to utilise online banking, as non-repudiation is primarily concerned with communication. Non-repudiation is a method that assures that clients (customers) are communicating with an authentic server (bank), and that none of the communication parties may subsequently falsely deny that the transaction had place. As a consequence, when compared to the other three elements, respondents consider that non-repudiation is the weakest component.

# CHAPTER 5

# DISCUSSION AND CONCLUSION

## 5.1 Introduction

This chapter present the summary of findings, discussions and conclusion of the study. This chapter starts with a recapitulation of the study followed by a section on the summary of the results of this research. The following section presents a discussion on the findings of this study. The fourth section presents the implications of the study which is divided into theoretical, methodological and practical contributions. Then, section five covers the limitations of the study followed by section six, which presents recommendation or suggestion for future research. Lastly, section seven presents the conclusion of this study and summarizes the whole chapter.

## 5.2 Key Findings

The goal of this research is to investigate the contributing impact of security factor towards internet banking usage in Malaysia. Internet banking is a system that enables users to conduct standard banking activities such as balance enquiries, money transfer between account, and utility bill payment without having to visit a bank. Internet banking consumers' perceptions of the talents, skills, and expertise of Internet banking services were classified in previous research as perceived competence (Normalini et al., 2019). The importance and relevance of security issues in customers' adoption of Internet banking has been widely recognised, and this has likely prompted internet security professionals to explore further on security factors. The findings of this study have some beneficial ramifications, particularly for the Malaysian banking sector, by providing beneficial insights for increasing online banking security and achieving ongoing usage by the consumer.

This study is quantitative research, which is this study aims to identify the important elements that influence the use of Internet banking by customers. There have been several studies undertaken in Malaysia and other countries that have documented the trend of increasing Internet banking use in Malaysia. This study also looks at the security factors that determine whether or not people will continue to use Internet banking services.

A total of 153 questionnaires were distributed to all internet banking users via Google Form. The majority of respondents were young aged adults, with almost 93.5% within the range of 20 to 29 years old. The remainder age less than 20 years (3.3%), 30 - 39 years (2.6%), and 40 - 49 years (0.7%). Statistical Package for the Social Sciences (SPSS) had generated and evaluated the data obtain (SPSS). There will be two steps to the data analysis. First before descriptive statistics technique by employ to evaluate the data, the first phase of the analysis did a descriptive statistical analysis to explored the data. Mean values, average scores, and comparative scores with each of the scales had been determined for each response. The following study based on these facts. Overall means, standard deviation, and skewness among data (person involve scores) for each factor had been computed, along with accurate system operations. After that, the data will be converted. Cronbach alphas will be use to check for content validity. Analyses were carried out based on the research framework, which was represented by the dependent variable (behavioural intentions) and the independent variable (perceived authentication, perceived confidentiality, perceived data integrity, and perceived non-repudiation).

Furthermore, reliability analysis were used in this study to determine the acceptance and validity of the questionnaire. Therefore, the surveyed questionnaire had been distributed to selected respondents who use internet banking in Malaysia. Cronbach's Alpha was used to determine whether the study was reliable or not. Cronbach Alpha which is one of the reliability tests conducted in SPSS. There are basically two alpha versions in the reliability analysis, namely the normal and standard versions. The normal version was used to measure the variables of this study for which the alpha normal version is typically used when items are scaled to produce a single score for that scale. The acceptable reliability value is .6. When the reliability result of the questionnaire is above 6 then your questionnaire is considered "reliable". In addition, the question was on a 5 -point Likert Scale with answers ranging from "Strongly agree" to "Strongly disagree". To determine whether the questionnaire can be "reliable" measure the variables. Thus, it is evident that Cronbach's Alpha has been able to measure the variables of interest accurately in this study. The statistics is considered applicable for further analysis.

The questionnaire development just as the unwavering reliability and validity of the instruments use in this investigation and measurement of variables and construct are remember for the sixth and seventh section individually. Section eight is given exclusively on plan of data analysis. At last, section nine gives the rundown of this section which is summary of the chapter. A questionnaire is lead to assemble the essential information for this quantitative research.

With the validity and reliability of the measurement model ascertained, the structural model was then evaluated to test the relationships hypothesised in this study. The study has four (4) hypotheses, as mentioned in Chapter 2. Hypotheses 1: Relationship of E-banking Usage Intention and Perceived Authentication. Hypotheses 2: Relationship of E-Banking Usage Intention and Perceived Confidentiality. Hypotheses 3: Relationship of E-Banking Usage Intention and Perceived Data Integrity. Meanwhile hypotheses 4 is  Relationship of E-Banking Usage Intention and Perceived Non-Repudiation.

## 5.3 Discussion

This study observed the impact of security factors towards e-banking usage intention in Malaysia. Base on the research framework, Technology acceptance model (TAM) and model of trust was used as origin. In detail, the discussion will focus on the research questions, and research objectives and hypotheses postulated in this study. Table 5.1 summarises the objectives, research question, assumptions and the finding of the study.

### 5.3.1 The relationship between perceived authentication and intention to use internet banking among Malaysia.

The initial research question examines whether perceived authentication relates to intention to use internet banking among Malaysia, the discussion of the hypothesis that answer the first question based on hypotheses testing (H1).

**Hypotheses 1: Perceived authentication has a positive relationship with E-banking usage intention**.

Finding of this study makes known a significant relationship between perceived authentication and E-banking usage intention among Malaysian. In comparison to a prior study, "Perceived Security Towards E-Banking Services: an examination among Malaysian young consumers” (Zaiton Osman, Azaze-Azizi Abdul Adis and Grace Phang et al., 2017) the results also show a significant relationship between perceived authentication and e-banking usage.

Since the result indicates that perceived authentication is significantly related to E-banking usage intention, this study's suggestion ratifies that perceived authentication is one of the most significant factors that Malaysian are concerns about security mechanisms while using e-banking. These findings give credence, and the researcher restrained the understanding of perceived authentication through fingerprints, response connections, encrypting, message authentication, screening firewalls, password management, hardware compatibility security, and card readers.

When it comes to perceived authentication, choosing stronger and unique passwords when registering for e-banking is the most significant factor to consider. This may seem self-evident, but even if you aren't aware of it, your password choice might provide an opportunity for hackers. Using personal information, such as your name, address, or date of birth, in your online banking passwords is one of the most prevalent blunders. Passwords are not updated on a regular basis, and 83 percent of online banking clients use the same password for several logins. (Cyclonis survey et al., 2018).

While doing so might help you remember your passwords, it also makes it simpler for hackers to guess your password and get access to your online banking information. There are some suggestions for making stronger passwords for online banking. Longer passwords, such as a phrase rather than a single word, including digits and special characters, are preferable. Use your name, your dogs' names, your date of birth, and other personal information sparingly. Your login information should not be saved in your online banking or mobile app.

When it comes to perceived authentication, choosing stronger and unique passwords when registering for e-banking is the most significant factor to consider. This may seem self-evident, but even if you aren't aware of it, your password choice might provide an opportunity for hackers. Using personal information, such as your name, address, or date of birth, in your online banking passwords is one of the most prevalent blunders. Passwords are not updated on a regular basis, and

83 percent of online banking clients use the same password for several logins. (Cyclonis survey et al., 2018).

While doing so might help you remember your passwords, it also makes it simpler for hackers to guess your password and get access to your online banking information. There are some suggestions for making stronger passwords for online banking. Longer passwords, such as a phrase rather than a single word, including digits and special characters, are preferable. Use your name, your date of birth, and other personal information sparingly. Your login information should not be saved in your online banking or mobile app.

### 5.3.2 The relationship between perceived confidentiality and intention to use internet banking among Malaysia.

The second research question concern the relationship between the perceived confidentiality towards e-banking usage intention among Malaysian. In detail, the discussion on hypotheses H2 will try to reaction the second research question. The discussion below touches on the findings of this study based on the research hypotheses.

**Hypotheses 2: Perceived confidentiality has a positive relationship with E-banking usage intention among Malaysia.**

Finding of this study makes known a significant relationship between perceived confidentiality and E-banking usage intention among Malaysian. In comparison to a prior study, "A Study on Attitude and Intention Towards Internet Banking with Reference to Malaysian Consumers in Klang Valley Region" (S. Arunkumar and Saranathan et al., 2012), the results also show a significant relationship between perceived confidentiality and e-banking usage.

Since the result indicates that perceived authentication is significantly related to E-banking usage intention, this study's suggestion by respect to the second question, this study demonstrated that the term "confidentiality" is employed to avoid data leak to unapproved elements, people or cycles. It alludes to security touchy and important property from unapproved revelation or block attempt. Privacy likewise implies that solitary verified gatherings or frameworks have the position to get to put away information. Information privacy could be penetrated either purposefully or inadvertently in various manners including hacking, phishing, email ridiculing and sending malignant code through email or both organizations.

Phishing is one of the most prevalent ways for identity thieves to steal personal and financial information. This type of fraud generally entails duping the scam victim into divulging personal information. Phishing scams may take many various forms, but email scams are the most common. For example, a scam victim may get an email that appears to be from their bank, instructing them to log in to their online account and update information.

The scam victim will click the link and log in to what looks to be a legitimate website but is actually a fake website. Alternatively, visiting a link instals tracking spyware on their machine, allowing identity thieves to log their keystrokes. As a result, any emails requesting money or personal information should be carefully scrutinised. First, look at the email's sender address. Then, rather of clicking on links, hover over them to see where the link text takes you. If the victim receives an email from their bank requesting information, they should phone the local branch or customer care to confirm that the email is authentic before providing any information.

### 5.3.3 The relationship between perceived data integrity and intention to use internet banking among Malaysia.

The third research question concern the relationship between the perceived data integrity towards e-banking usage intention among Malaysian. In detail, the discussion on hypotheses H3 will try to reaction the third research question. The discussion below touches on the findings of this study based on the research hypotheses.

**Hypotheses 3: Perceived data integrity has a positive relationship with E-banking usage intention among Malaysia.**

In response to the third question, finding of this study makes known a significant relationship between perceived data integrity and E-banking usage intention among Malaysian. In comparison to a prior study, "Investigating the Impact of Security Factor In E-Banking and Internet Banking Usage Intention Among Malaysians," (Normalini, Muhammad Salman Shabbir, and T. Ramayah et al., 2019) the results also show a significant relationship between perceived and e-banking usage.

This research revealed It's important to note that changing data is totally acceptable. Modifications and updates are permissible as long as they are consistent across systems and storage. When unforeseen changes occur, the issue emerges. Data corruption may occur in a variety of ways, but it usually falls into one of two categories: technical faults and security weaknesses.

Technical problems can arise in both software and hardware. Technical mistakes have a direct impact on data during storage and transmission. Data can be rendered worthless if it is changed or deleted. It is no longer usable by systems since it has changed from its original form. One of the most prevalent and significant risks to data integrity is security issues.

By hacking into databases and disrupting communication, cybercriminals want to disrupt systems and profit financially. The WannaCry ransomware assault in 2017 is an excellent example. Because of its ramifications across several businesses, it is classified as a data breach. It encrypts the information, rendering it worthless. The cost of the destruction was estimated to be in the billions of dollars throughout the world.

### 5.3.4 The relationship between perceived Non-repudiation and intention to use internet banking among Malaysia.

The fourth research question concern the relationship between the perceived Non-repudiation towards e-banking usage intention among Malaysian. In detail, the discussion on hypotheses H4 will try to reaction the fourth research question. The discussion below touches on the findings of this study based on the research hypotheses.

**Hypotheses 4: Perceived Non-repudiation has a positive relationship with E-banking usage intention among Malaysia**.

Finding of this study makes known a significant relationship between perceived Non-repudiation and E-banking usage intention among Malaysian. In comparison to a prior study, "Perceived Ease of Use and Trust Towards Intention to Use Online Banking in Malaysia" (Nur Shafini Mohd Said & Suhaily Maizan Abdul Manaf et al., 2020) the results also show a significant relationship between perceived Non-repudiation and e-banking usage.

By respect to the fourth question, this study demonstrated that Non-repudiation is a feature that ensures customers that they are communicating with a genuine person (bank), or the other way around, to such an extent that neither of the conveying gatherings can later dishonestly reject that the exchange occurred. Banks maintain and regularly update exchange logs, which contain a variety of information such as the nature, time, and date of customers transactions. These records allow for the verification of all sorts of transactions done and offer the necessary documentation in the event of a problem.

When utilising online banking, we may sign up for banking notifications to acquire the information we need. One of the simplest methods to stay on top of your financial activities and check security is to use banking alerts and notifications. You may be able to enrol in email or SMS alerts to receive updates depending on how your bank operates. Notifications for new credit and debit transactions, unsuccessful login alerts, password change alerts, and outbound wire transfer alerts are all examples of alerts you might wish to set up. Notifications can also help if your account is hacked and a fraudulent transaction is made.

## 5.4 Implications of the Study

The findings of this research provide some valuable implications especially for the banking industry in Malaysia by offering useful insights for improving internet banking security and attain continuous usage by customers. From users' perspective, security dimensions of authentication and perceived confidentiality were found significant in developing users' intention to continue usage of Internet banking.

These findings of the study are advantageous for the banks and provide empirical evidence of perceived importance of authentication and confidentiality, which will help banks to design their internet banking with these security dimensions. Financial organisations considering using e-banking systems should analyse and research the individual features of possible users in the geographic areas where the technology will be implemented. Banks must emphasise the factors that consumers evaluate when deciding whether or not to use internet banking. This research aids banks in identifying key criteria for offering more complete and sufficient internet banking services to the public. Many banks are developing their respective strategies or policies that can provide user-friendly and acceptable online banking services; nevertheless, they must consider comprehensive internet banking services that can provide their customers complete trust. Some institutions are still lagging behind in terms of delivering safe and secure online banking. As a result, Malaysia's online banking systems can yet be improved. This will aid them in comprehending the impact that these characteristics may have on customers' propensity to embrace and employ technology.

Furthermore, the study also aimed at highlighting the role and importance of authentication, perceived confidentiality, and perceived data integrity in order to improve, refine, and implement internet banking security and ultimately achieve continuous Internet usage. Therefore, to improve customer trust, banks may help them by creating safe online banking processes and risk management procedures. Customers should be able to readily contact with employees who are well-trained in problem-solving and, as a result, have strong customer orientations. Furthermore, banks must emphasise the advantages of online banking by making it simple to use and enhancing security, in order to increase client trust. It's also critical that they promote and advertise the advantages of internet banking (Khalil et al., 2010). Customers of all backgrounds and cultures may be encouraged to continue using online banking as a result of this (Ahmed, Islam and Yahya, 2014).

## 5.5 Limitations of the Study

This study has several limitations, which must be considered when interpreting the study's findings and its implications.

First, the study was focused to empirically investigate the contributing impact of security factor towards banking usage in Malaysia. Furthermore, this study focused on the customer's intention which is only from the users of the E-banking in Malaysia.

Second, the difficulty encountered while collecting the questionnaire data for this study is that it takes a long time to achieve the desired target of 153 people. The obstacle we faced while collecting the data of this questionnaire was not everyone was diligent enough to take the time to answer the questionnaire.

Third, respondents' impressions of perceived authentication, perceived confidentiality, perceived data integrity, perceived non-repudiation, and customer intention were collected using the survey instrument. As a result, like other research that employ a survey instrument, it's possible that the results will be skewed.

## 5.6 Recommendations/ Suggestion for Future Research

Each study has its own set of restrictions, yet the each research endeavour provides new specialty results that serve as the foundation for future research. As a result, this section looks at the field of research that might be investigated in the future.

Perceived authentication, perceived confidentiality, perceived data integrity, and perceived non-repudiation were all investigated as aspects of security in order to uncover characteristics that might impact the intention to continue using Internet banking. As a result, it is anticipated that this online banking security model would spark new debate about the numerous issues about internet banking security. However, further research is needed to identify the most important online banking security antecedents.

To begin, further study in the field of internet banking security in Malaysia is recommended to further examine the determinants of internet banking security and provide a complete model in order to add to the literature in the subject. Furthermore, specific efforts may be made to establish which aspects of security contribute to unfavourable attitudes regarding online banking, as well as how attitudes might be modified to increase internet banking usage intention. The banking sector might use the findings of this study to build online banking security features that react to the unique demands of clients, resulting in more positive attitudes toward internet banking.

Second, while this study included important variables, future studies could include additional variables such as perceived accessibility and perceived awareness that could be useful in determining the widespread use of internet banking. Subsequently, studies should include more independent variables to assess people's perceptions of internet banking. Furthermore, the study is based on TAM, which was recommended and validated using the Cronbach Alpha approach in

SPSS. Future research should focus on consumer behaviour in relation to other ideas on technology adoption and acceptance. Future research in the context of mobile banking adoption in Malaysia or any other nation should include some more relevant elements.

Finally, future research might expand on this study by incorporating business clients and students, allowing for comparisons between various groups' decisions and criteria for adopting online banking services. Additionally, researchers can expand the number of participants and gather data over a longer period of time. Most crucially, the limited sample size (150 responders) may have resulted in inconsistencies in the results. A bigger sample that approaches the population size and includes all of the population's features should reduce sampling process error and yield more reliable results.

## 5.7 Overall Conclusion of the Study

The main goal of this research is to empirically investigate the impact of security factors on internet banking usage in Malaysia in order to determine whether or not people will continue to use the service. Two theories are used to explain the findings in this study to achieve the proposed objective: the Technology Acceptance Model (TAM) and the Model of Trust. It has five variables: a dependent variable (behavioural intention) and four independent variables (perceived authentication, perceived confidentiality, perceived data integrity and perceived non repudiation). The quantitative analytical approach that was used in this study, on the other hand.

The suggested model effectively presents several important results, such as the fact that once Internet banking users in Malaysia have trust in the trustworthiness of Internet banking, they may feel more comfortable doing financial transactions online using Internet banking. Overall, the results show that most of the hypotheses tested have a high statistical significance, and the findings of the data obtained have been recognised and analysed.

This investigation had now been completed morally and with a great deal of dedication. By directing this research, it also adhered to all of the rules and regulations. Without a doubt, the goal of this study was to provide useful information and statistics to all users in order to assist them with comparing issues.

# REFERENCES

Abdelghani Echchabi, Salim Al-Hajri & Islam Nazier Tanas (2019). Analysis of E-Banking Acceptance in Oman: The Case of Islamic Banks’ Customers. IJIEF: International Journal of Islamic Economics and Finance Vol. 1 (2), page 145-164, January 2019.

Abdel Latef M. Anouze and Ahmed S. Alamro (2020). Factors affecting intention to use e-banking in Jordan. International Journal of Banking Marketing, Page 86 - 112, Vol 38, No. 1, 2020.

Ali Hussein Abu Zaid, Norhidayah Azman and Nurdiana Azizan (2020). Success Factors Consideration for E-banking Web site from User Perspectives in Malaysia: A Study Using the Knowledge. Journal of Global Scientific Research, Page 295 -306, 5 May 2020.

Ahmad Ali Harasis and Amran Rasli (2016). A Review of Theories Relevant to E-banking Usage Continuance. International Review of Management and Marketing, 2016, 6(S4) 277-283.

Ayana Gemechu Bultum (2014). Factors Affecting Adoption of Electronic Banking System in Ethiopian Banking Industry. Journal of Management Information System and E-commerce, Vol. 1, No. 1; June 2014.

Bestoon Othman, Amran Harun, Darbaz Answer Ismail, Zana Majed Sadq, Sher Ali and Thomas Stephen Ramsey (2019). Malaysian Consumer Behaviour towards Internet Banking: An Application of Technology Acceptance Model. International Journal of Psychosocial Rehabilitation, Vol. 23, Issue 02, 2019.

Chong Hui Ling, Md. Aminul Islam, Arman Hadi Abdul Manaf and Wan Mashumi Wan Mustafa (2015). Users Satisfaction Towwards Online Banking in Malaysia. International Business Management, Vol. 9, Issue 1, 2015.

Fazlan Abdullah, Nadia Salwa Mohamad and Zahri Yunos (2018). Safeguarding Malaysia’s Cyberspace against Cyber Threats: Contributions by CyberSecurity Malaysia. OIC-CERT Journal of Cyber Security, Page 22 – 31, 2018.

F B Fatokun, S. Hamid, A. Norman and J. O. Fatokun (2019). The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. International Conference Computer Science and Engineering, October 2019.

Hema Raviadaran, Omkar Dastane, Muhamad Yusnorizam Ma’arif & Nurhizam Safie Mohd Satar (2019). Impact of Service Quality Dimensions on Internet Banking Adoption, Satisfaction and Patronage. International Journal of Management, Accounting and Economics, Vol. 6, No. 10, October 2019.

Jacquline Thami, Mohd Shukri Ab Yazid, Abdol Ali Khatibi and S. M. Ferdous Azam (2017). Internet and Data Security – Understanding Customer Perception on Trusting Virtual Banking Security in Malaysia. European Journal of Social Sciences Studies, Vol 3, Issue 7, 2017.

Lin L (2018), Factors Influencing the Behaviour Intention of E-Banking Transactions Through Mobile Phones in China. Journal of Internet Banking and Commerce, vol. 23, no. 1, April 2018.

Mahiswaran Selvanathan, Rubana Vighnesvaran, Voon Ying Teng and Faria Rabbi (2016). Internet Banking Challenges among Customers in Selangor, Malaysia. International Journal of Human Resource Studies Vol. 6, Issue 3. 2016.

Martin Vejačka, Tomáš Štofa (2017), Influence of Security and Trust on Electronic Banking Adoption in Slovakia. JEL Classifi cation: G29, L86. DOI: 10.15240/tul/001/2017-4-010.

Maryam Sohrabi, Julie Yew Mei Yee & Robert Jeyakumar Nathan (2012). Critical Success Factor for the Adoption of e-Banking in Malaysia. International Arab Journal of e-Technology, Vol. 3, No. 2, June 2013.

Mathavi Massilamany and Dineswary Nadarajan (2017). Factors That Influencing Adoption of Internet Banking in Malaysia. International Journal of Business and Management; Vol. 12, No. 3, 2017.

Md Arif Hassan, Zarina Shukur, Mohammad Kamrul Hasan and Ahmed Salih Al-Khaleefa (2020). A Review on Electronic Payments Security. Symmetry 12 August 2020, 1344; doi:10.3390/ sym12081344.

Murat Mahad, Shahimi Mohtar and Abdul Aziz Othman (2015). The Effect of Perceived Trust of Mobile Banking Services in Malaysia. International Academic Research Journal of Business and Technology, Page 1 – 7, Vol 1, Issue 2, 2015.

Nur Hazwani Abdul Aziz & Nuradli Ridzwan Shah Mohd Dali (2019). Factors Influencing Consumer Behavior Towards the Usage of Internet Banking. IJASOS- International E-Journal of Advances in Social Sciences, Vol. V, Issue 14, August 2019.

Normalini M.K., T. Ramayah & Muhammad Salman Shabbir (2019). Investigating the Impact of Security Factors In E-business and Internet Banking Usage Intention among Malaysians. Industrial Engineering & Management Systems,Page 501 – 510, Vol. 18, No. 3, September 2019.

Normalini M.K. and T. Ramayah (2017). Trust in Internet Banking in Malaysia and the Moderating Influence of Perceived Effectiveness of Biometrics Technology on Perceived Privacy and Security. Journal of Management Sciences, Vol. 4 Issue 1, Page 3-26, 2017.

Pallab Sikdar, Amresh Kumar & Munish Makkad (2015). Online banking adoption: A factor validation and satisfaction causation study in the context of Indian banking customers. International Journal of Bank Marketing, September 2015.

Santos Marianus and Syaiful Ali (2021), Determining Factors of the Perceived Security Dimensions in B2C Electronic Commerce Website: An Indonesian Study. Journal of Accounting and Investment, Vol. 22 No. 1, January 2021.

Siti Rapidah Omar Ali1, Wan Nur Khadijah Wan Marzuki2, Nur Shafini Mohd Said, Suhaily Maizan Abdul Manaf and Nur Dalila Adenan (2020). Perceived Ease of Use and Trust Towards Intention to Use Online Banking in Malaysia. Jurnal Intelek, Vol. 15, Issue 1, February 2020.

Syuhaily Osman and Tan Pik Leng (2020). Factors Influencing Behavioural Intention for Mobile Banking Adoption Among Students of Universiti Putra Malaysia. Malaysian Journal of Consumer and Family Economics Vol 24, 2020.

Teju Kujur & Mushtaq Ahmad Shah (2015). Electronic Banking: Impact, Risk and Security Issues. International Journal of Engineering and Management Research, Page 207 – 212, Volume-5, Issue-5, October 2015.

TIPI, Lucian, XIAO, Yan, SUKUNAR, Arun and EDGAR, David (2017). Factors Influencing People’s Intention to Adopt E-Banking: An Empirical Study of Consumers in Shandong Province, China. Asian Journal of Computer and Information Systems, Vol. 5, Issue 3, October 2017.

Viknesh Venkathaialam and Abdulkadir Shehu Abdulwahab (2017). The Impact of Digitalization of Retail Banks in Malaysia on Customer Experience. International Journal of Accounting & Business Management, Vol. 5, No.2, November 2017.

Wan-Shin Ho and Sofri Yahya (2015). Consumers’ perception towards the extent of internet banking usage in Malaysia. Problems and Perspectives in Management, vol. 13, issue 2, 2015.

Yong Hoe Hong, Boon Heng The, Gowrie Vinayan, Chin Hooi Soh, Nasreen Khan & Tze San Ong (2013). Investigating the Factors Influence Adoption of Internet Banking in Malaysia: Adopters Perspective. International Journal of Business and Management; Vol. 8, No. 19, 2013.

Yousuf Salim Alhinai, Ali Albadi, Hafedh Alshihi & Khamis Al-Gharbi (2013). Investigating Determinants of E-banking Adoption by Individuals: Comparing the Impact of System Characteristics and User Traits. International Review of Management and Business Research Vol. 2, Issue. 2; June 2013.

Zahoor Ur Rehman, Siti Sarah Binti Omar, Shafie Bin Mohamad Zabri & Sonia Lohana (2019). Mobile Banking Adoption and its Determinants in Malaysia. International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-1, November 2019.

Zahoor Ur Rehman and Fazal Ali Shaikh (2020). Critical Factors Influencing the Behavioral Intention of Consumers towards Mobile Banking in Malaysia. Engineering, Technology & Applied Science Research Vol. 10, No. 1, 2020, 5265-5269.

Zaiton Osman, Azaze-Azizi Abdul Adis & Grace Phang (2017). Perceived Security Towards E-Banking Services: An Examination Among Malaysian Young Consumers. Journal of the Asian Academy of Applied Business, Vol. 4, December 2017.

Zhong Zhao, Yue Lan and Xiaoyu Wu (2016). The Impact of Electronic Banking on the Credit Risk of Commercial Banking. Journal of Mathematical Finance, Page 778 – 791, Vol. 6, 2016.

## APPENDIX A

## QUESTIONNAIRE DRAFT

### Section A: Respondents' Profile

| | |
|---|---|
| 1. Age | i. Below 20 years<br>ii. 20-29 years<br>iii. 30-39 years<br>iv. 40-49 years<br>v. 50 years and above |
| 2. Gender | i. Male<br>ii. Female |
| 3. Race | i. Malay<br>ii. Chinese<br>iii. Indian<br>iv. Others |
| 4. Education Level | i. SPM<br>ii. STPM<br>iii. Certificate<br>iv. Diploma<br>v. Degree or higher |
| 5. Employment Status | i. Student<br>ii. Self-employed<br>iii. Private Sector<br>iv. Government Sector<br>v. Others |
| 6. Income | i. Below RM2500<br>ii. RM2501 – RM4850<br>iii. RM4851 – RM10970<br>iv. RM10971 and above |
| 7. Usage of Internet | i. Below 3 years<br>ii. 3-5 years<br>iii. 7-11 years<br>iv. 12-15 years<br>v. 16 years and above |
| 8. Usage of E-banking | i. Below 1 year<br>ii. 1-10 years<br>iii. 11-20 years<br>iv. 20 years and above |
| 9. Primary Place of Internet Banking | i. Home<br>ii. Office<br>iii. Internet café<br>iv. Others |

**Section B: Intention to use E-Banking**

| Items | Measured items | Strongly disagree | Disagree | Neutral | Agree | Strongly agree |
|---|---|---|---|---|---|---|
| 1. | I intend to continue using Internet banking services rather than discontinue its use. | 1 | 2 | 3 | 4 | 5 |
| 2. | My intentions are to continue using Internet banking services than use any alternative means (traditional banking). | 1 | 2 | 3 | 4 | 5 |
| 3. | I intend to continue using Internet banking services whenever I need it. | 1 | 2 | 3 | 4 | 5 |
| 4. | I intend to continue using Internet banking service feature since it is good. | 1 | 2 | 3 | 4 | 5 |

**Section C: Perceived Authentication**

| Items | Measured items | Strongly disagree | Disagree | Neutral | Agree | Strongly agree |
|---|---|---|---|---|---|---|
| 1. | The transactions I send are transmitted to my Internet banking site. | 1 | 2 | 3 | 4 | 5 |
| 2. | The messages I receive are transmitted from my Internet banking site. | 1 | 2 | 3 | 4 | 5 |
| 3. | My Internet banking site ascertains my identity before sending any messages to me. | 1 | 2 | 3 | 4 | 5 |
| 4. | My Internet banking site ascertains my identity before processing the transaction received from me. | 1 | 2 | 3 | 4 | 5 |

**Section D: Perceived Confidentiality**

| Items | Measured items | Strongly disagree | Disagree | Neutral | Agree | Strongly agree |
|---|---|---|---|---|---|---|
| 1. | All the communication with my Internet banking site are strictly within the site and me. | 1 | 2 | 3 | 4 | 5 |
| 2. | I am convinced that my Internet banking site respects the confidentiality of the transactions received from me. | 1 | 2 | 3 | 4 | 5 |
| 3. | My Internet banking site uses some security controls for the confidentiality of the transactions. | 1 | 2 | 3 | 4 | 5 |
| 4. | My Internet banking site checks all communications between the site and me for the protection from wiretapping or eavesdropping. | 1 | 2 | 3 | 4 | 5 |

**Section E: Perceived Data Integrity**

| Items | Measured items | Strongly disagree | Disagree | Neutral | Agree | Strongly agree |
|---|---|---|---|---|---|---|
| 1. | My Internet banking site checks the information communicated with me for accuracy. | 1 | 2 | 3 | 4 | 5 |
| 2. | My Internet banking site takes steps to make sure that the information in transit is accurate. | 1 | 2 | 3 | 4 | 5 |
| 3. | My Internet banking site takes steps to make sure that the information in transit is not deleted. | 1 | 2 | 3 | 4 | 5 |
| 4. | My Internet banking site devotes time and effort to verify the accuracy of the information in transit. | 1 | 2 | 3 | 4 | 5 |

**Section E: Perceived Non-Repudiation**

| Items | Measured items | Strongly disagree | Disagree | Neutral | Agree | Strongly agree |
|---|---|---|---|---|---|---|
| 1. | My Internet banking site will not deny having participated in a transaction after processing it. | 1 | 2 | 3 | 4 | 5 |
| 2. | My Internet banking site will not deny having received a transaction from me. | 1 | 2 | 3 | 4 | 5 |
| 3. | My Internet banking site will not deny having sent me a message. | 1 | 2 | 3 | 4 | 5 |
| 4. | My Internet banking site provides me with some evidence to protect against its denial of having received a transaction from me. | 1 | 2 | 3 | 4 | 5 |

# APPENDIX B

## GANTT CHART

| SEMESTER 6 | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ACTIVITIES** | | **W1** | **W2** | **W3** | **W4** | **W5** | **W6** | **W7** | **W8** | **W9** | **W10** | **W11** | **W12** | **W13** | **W14** | **W15** |
| 1 | Introduction | 🟩 | 🟩 | 🟩 | | | | | | | | | | | | |
| 2 | Literature Review | | | | 🟩 | 🟩 | 🟩 | 🟩 | | | | | | | | |
| 3 | Research Methodology | | | | | | | | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | |
| 4 | Draft of Questionnaire | | | | | | | | | | | | | 🟩 | 🟩 | 🟩 |
| **SEMESTER 7** | | | | | | | | | | | | | | | | |
| **ACTIVITIES** | | **W1** | **W2** | **W3** | **W4** | **W5** | **W6** | **W7** | **W8** | **W9** | **W10** | **W11** | **W12** | **W13** | **W14** | **W15** |
| 5 | Data Collection | 🟩 | 🟩 | | | | | | | | | | | | | |
| 6 | Data Recording, Monitoring, and Analysis | | | 🟩 | 🟩 | 🟩 | 🟩 | | | | | | | | | |
| 7 | Discussion and Conclusion | | | | | | 🟩 | 🟩 | 🟩 | 🟩 | | | | | | |
| 8 | The Model Developed | | | | | | | | | 🟩 | 🟩 | 🟩 | | | | |
| 9 | Report and Documentation | | | | | | | | | | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| 10 | Completion of Report and Documentation | | | | | | | | | | | | | | | 🟩 |