Analysing the Security and Usability of Online Banking Applications in Pakistan

By

Muneeba Darwaish

(Registration No: 00000273612)

Supervisor: Dr. Sana Qadir

Department of Information Security, Computer Science

School of Electrical Engineering and Computer Science (SEECS)

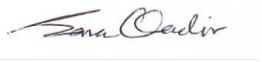
National University of Science & Technology (NUST)

Islamabad, Pakistan

(2022)

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis entitled "Analysing the Security and Usability of Online Banking Applications in Pakistan" written by Muneeba Darwaish, (Registration No 00000273612), of SEECS has been vetted by the undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: 

Name of Advisor: Dr. Sana Qadir

Date: 29-Jun-2022

HoD/Associate Dean: _____

Date: _____

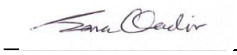
Signature (Dean/Principal): _____

Date: _____

Approval

It is certified that the contents and form of the thesis entitled "Analysing the Security and Usability of Online Banking Applications in Pakistan" submitted by Muneeba Darwaish have been found satisfactory for the requirement of the degree

Advisor : Dr. Sana Qadir

Signature: 

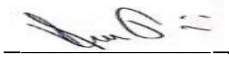
Date: 29-Jun-2022

Committee Member 1:Dr. Mehdi Hussain

Signature: 

29-Jun-2022

Committee Member 2:Dr. Dr Hasan Tahir

Signature: 

Date: 29-Jun-2022

Signature: _____

Date: _____

DEDICATION

All of my hard work is dedicated to my parents, who have supported me throughout my career, my siblings, and my friends, who have inspired and supported me throughout my tough times.

Certificate of Originality

I hereby declare that this submission titled "Analysing the Security and Usability of Online Banking Applications in Pakistan" is my own work. To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics, which has been acknowledged. I also verified the originality of contents through plagiarism software.

Student Name:Muneeba Darwaish

Student Signature: 

ACKNOWLEDGEMENT

Alhamdulillah! Allah has blessed me throughout my life and has given me the strength to complete my thesis at every stage. I am pleased to have kind and supportive parents and siblings. I am grateful for their consistent support and prayers, which have helped me to stay focused and dedicated to achieving all of my objectives.

I would like to express my gratitude to Dr. Sana Qadir, my very supportive supervisor, who has always been available to me, guided me down this path and provided me with vital input at every level of my research. I am extremely grateful to my GEC members, Dr. Hasan Tahir and Dr. Mehdi Hussain, for their guidance, assistance, advice, and comments, in finishing my work and delivering excellent research.

TABLE OF CONTENTS

Page No.

CHAPTER 1: INTRODUCTION **1**
1.1 Security **3**
1.2 Usability **4**
1.3 Problem Statement **6**
1.4 Purpose of Study **7**
1.5 Research Questions **7**
1.6 Scope **8**
1.7 Limitations of the Study **9**
1.8 Advantages and Disadvantages of Online Banking **9**
1.9 Target Group **10**
1.10 Application **10**
CHAPTER 2: LITERATURE REVIEW **11**
2.1 Background Concepts **11**
2.1.1 Online Banking 11
2.1.2 Online Banking in Pakistan 13
2.1.3 Types of Online Banking 13
2.2 Related Work **14**
2.2.1 Review of Studies on Security of Online Banking 14
2.2.2 Review of Studies on Usability of Online Banking 15
2.2.3 Review of Studies on Usability and Security of Online Banking 16
CHAPTER 3: RESEARCH METHODOLOGY **19**
3.1 Workflow **19**
3.2 Topic Selection **20**
3.3 Theory Selection **20**
3.4 Research Process **21**
3.4.1 Research Method 21
3.4.2 Relationship between Quantitative and Qualitative Approach 21

3.4.3 Interview Participants Information 22
3.4.4 Quantitative Approach 22
3.4.4.1 Design of Survey for Users 23
3.4.4.2 Sampling Technique 24
3.4.4.3 Data Collection 24
3.4.4.4 Data Analysis 24
3.4.4.5 Interpretation of Findings 24
3.4.5 Qualitative Approach 25
3.4.5.1 Design of Interview for Experts 25
3.4.5.2 Sampling Technique 26
3.4.5.3 Data Collection 26
3.4.5.4 Data Analysis 26
3.4.5.5 Interpretation of Findings 26
3.4.6 Primary Data 26
3.4.6.1 Survey and Interview Methods 27
3.4.6.2 Questionnaire/Interview Methodology 27
3.4.6.3 Survey Format 28
3.5 The research's validity and reliability 28
CHAPTER 4: RESULTS AND ANALYSIS 30
4.1 Survey 30
4.1.1 Demographic Information 30
4.1.2 Users and Non-Users 34
4.1.3 Reasons for not using online banking 35
4.1.4 General Information 37
4.1.5 Usability Analysis 41
4.1.6 Security Analysis 52
4.1.7 Comparison with International Online Banking 70
4.2 Summary of Hypothesis Testing 86
4.3 Summary of Usability-related Hypothesis 87
4.4 Summary of Security-related Hypothesis 88
4.5 Interview 89
4.6 Discussion of the Results 100

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS 103
5.1 Conclusion 103
5.2 Recommendations 106
5.3 Future Work 107
REFERENCES 108
APPENDIX A ..... a

LIST OF ABBREVIATIONS

CA	Certificate Authority
DFIs	Development Finance Institutions
ETGRF	Enterprise Technology Governance and Risk Management Framework
ECC	Elliptic Curve Cryptography
E-Banking	Electronic Banking
FIs	Financial Intermediaries
GDPR	General Data Protection Regulation
HCI	Human-Computer Interaction
IMEI	International Mobile Equipment Identity
PKI	Public Key Infrastructure
MFA	Multi-Factor Authentication
NFC	Near Field Communication Technology
OB	Online Banking
OTP	One Time Password
PCI-DSS	Payment Card Industry Data Security Standard
QR	Quick Response
SSL	Secure Sockets Layer
SPSS	Statistical Package for the Social Sciences
SFA	Single Factor Authentication
SBP	State Bank of Pakistan
TAM	Technology Acceptance Model
TPB	Theory of Planned Behaviour
UI	Users Interface
UX	Users Experience

LIST OF TABLES

Page No.

Table 3.1: Design of Survey 23
Table 3.2: Design of Interview 25
Table 4.1: Hypothesis 1(a) 34
Table 4.2: Hypothesis 1 (b) 36
Table 4.3: Hypothesis 2 (a) 44
Table 4.4: Hypothesis 2 (b) 48
Table 4.5: Hypothesis 2 (c) 51
Table 4.6: Hypothesis 3 (a) 58
Table 4.7: Hypothesis 3 (b) 61
Table 4.8: Hypothesis 3 (c) 63
Table 4.9: Usability Analysis of International Online Banking Applications 73
Table 4.10: Security Analysis of International Online Banking Applications 75
Table 4.11: User Education Analysis of International Online Banking Applications 78
Table 4.12: Hypothesis 4 (a) 80
Table 4.13: Hypothesis 4 (b) 83
Table 4.14: Hypothesis Summary 86
Table 4.15: Summary of Usability-related Hypothesis 87
Table 4.16: Summary of Security-related Hypothesis 88
Table 4.17: Interview Responses for Question on Usability 89
Table 4.18: Responses for Question 1 on security 91
Table 4.19: Responses for Question 2 on Security 92
Table 4.20: Responses for Question 1 on Usability and Security 93
Table 4.21: Responses for Question 2 on Usability and security 94
Table 4.22: Responses for Question 1 on User Education 95
Table 4.23: Responses for Question 2 on User Education 96
Table 4.24: Responses for Question 3 on User Education 97
Table 4.25: Responses for Question on Comparison between Pakistani and International Online Banking Services 98
Table 4.26: Responses for Question on Suggestions for Improvement 99
Table 4.27: Usability Results of Survey and Interview 100
Table 4.28: Security Results of Survey and Interview 101
Table 4.29: User Education Results of Survey and Interview 101
Table 4.30: Comparison between Pakistani and International Online Banking Applications 102

List of Figures

Page No.

Figure 2.1: Online Banking Model [41] 12
Figure 3.1: Thesis Work Flow 19
Figure 3.2: Quantitative and Qualitative Approach 21
Figure 4.1: Respondents' Gender 31
Figure 4.2: Respondents' Age 31
Figure 4.3: Respondents' Education 32
Figure 4.4: Respondent's Computer Expertise 32
Figure 4.5: Respondent's Computer Security Expertise 33
Figure 4.6: Respondents' Nationality 33
Figure 4.7: Users and Non-Users 34
Figure 4.8: Reasons for Not Using Online Banking 35
Figure 4.9: Service Providers 37
Figure 4.10: Frequency of Using Online Banking Applications 38
Figure 4.11: Commonly Use Applications 39
Figure 4.12: Control over Online Banking 40
Figure 4.13: Availability of Guidance /Manual/ Help Features 41
Figure 4.14: Guidance/Help Features Usefulness 42
Figure 4.15: Familiarity with Features / Functions 43
Figure 4.16: Difficulties / Problems 45
Figure 4.17: Memorability Features 46
Figure 4.18: Error Reporting Features 47
Figure 4.19: Complicated for Non-technical Users 49
Figure 4.20: Authentication Features Limit Users 50
Figure 4.21: Service Provider Web Address 52
Figure 4.22: Mostly Used Authentication Mechanism 53
Figure 4.23: Same Password for Different Applications 54
Figure 4.24: Password Verification for Different Applications 55
Figure 4.25: Additional Authentication Requirement 56
Figure 4.26: Additional Authentication Needed 57
Figure 4.27: Security-Related Information 59
Figure 4.28: Familiarity with Security Features 60
Figure 4.29: Convenience or Security 62
Figure 4.30: Concerned About the security 64
Figure 4.31: Best Security Measures 65
Figure 4.32: Unwanted Security Features 66

Figure 4.33: Feel Secure While Banking Online 67
Figure 4.34: Satisfaction with Security Features 68
Figure 4.35: Advanced Authentication Methods 69
Figure 4.36: Foreign Online Banking Application Users 71
Figure 4.37: Foreign Countries/ Banks Name 72

ABSTRACT

The smartphone and the internet have become an intrinsic part of our lives. In the current era, people mostly rely on smartphones to perform their tasks with convenience and efficiency. A lot of applications are available to facilitate users. Among all these applications, online banking applications are also gaining popularity in Pakistan. As a result of COVID-19, a lot of users in Pakistan switched to online banking. However, the most significant obstacles to the widespread use of online banking applications are security and usability concerns.

The goal of this research is to analyse the security and usability of online banking applications in Pakistan. An investigation of security, usability, users' education, and comparison with international online banking applications is carried out in this study. An online survey was used to collect users' perspectives on security and usability issues in online banking. To better understand the survey results interviews sessions were conducted. Survey and interview findings were compared to highlight the strengths and weaknesses of online banking applications in Pakistan.

It is hoped that the findings of this thesis will help online banking service providers in Pakistan to recognize usability, security, and user education issues and make their services more secure, usable, and convenient. Additionally, this study aims to identify users' needs and provide suggestions for improving the acceptance and usage of online banking applications in Pakistan.

Keywords: Security, usability, users' education, comparison

CHAPTER 1: INTRODUCTION

Online banking is gaining more popularity in Pakistan, especially during the COVID-19 pandemic. Because of the extensive usage of the internet, almost all organizations now offer online services to their customers. Banks, like other organizations, offer online services to their consumers. As banks are dealing with sensitive information, **security** and **usability** are the two biggest concerns about online banking.

The purpose of this dissertation is to examine the security and usability of online banking applications in Pakistan. Users of online banking have access to a variety of handy banking services. The motivation of users to use online banking is influenced by security and usability. People are scared of using online banking due to security and usability concerns. In online banking, end-users face major challenges, especially with technical terms, security features, usability, and other technical issues [1].

Security-related materials might sometimes be too technical for laymen users to understand. End-users, especially those with a non-technical background, can be confused by terms like "digital signature," "verify," and "authentication". Security concerns are one of the key factors that have been identified as impeding the growth and adoption of online banking services [4].

Usability is one of the most important factors to consider when evaluating the quality of online banking services. In online banking, a poorly designed interface of applications can lead to many unexpected problems. If the online banking system interface is too complicated and restrictive, authorized users will face difficulty using it.

The level of security is typically determined by the strength of the authentication techniques used in online banking. Customers use authentication to gain access to their personal and sensitive data. Banks should provide their customers with secure and simple authentication procedures; otherwise, the authentication procedure may become counter-productive and inconvenient for users [2]. Customers' intentions to continue using online banking are positively influenced by authentication mechanisms. Unauthorized access, reputational damage through fraud, financial loss, identity theft, and disclosure of customer information can all be avoided with an effective, secure, and usable authentication system. Striking a balance between security and user experience in mobile apps and web banking is becoming increasingly difficult for online banking service providers [3].

Users can make financial transactions over the Internet with the help of online banking. Anyone, from any location, at any time can access online banking services. Most conventional bank services, such as bill payment, viewing account information, and financial management, are available through online banking. Online banking services can be accessed by a computer, a mobile phone, or a smartphone.

Even though online banking has resulted in substantial improvements across banks in terms of rapid service engagement and service delivery, the same aspects of online banking security remain problematic [1]. The most significant problems while using online banking

services are related to security and usability. People are hesitant to use online banking services because of such issues [11].

Security and usability are the two most important considerations in online banking. Usability is determined by five factors: efficiency, memorability, learnability, error prevention, and satisfaction. Security is determined by two of the most important factors: safety and privacy. Users prefer more conventional and familiar technologies, such as fingerprint or facial recognition, over approaches that are slightly more intangible, such as typing or gait analysis, in terms of usability [7].

1.1 Security

The most important consideration in online banking is security. The goal of online banking security is to make users feel safe and secure. Security features are designed to give a shield or protection. The two most commonly used components of security are:

Safety: The feeling of being safe comes from knowing that you are shielded from the things that can hurt you.

Privacy: Privacy is a type of security that allows a person or a group to keep personal information private and express themselves selectively.

Individuals, organizations, and institutions have the right to decide when, how, and to what degree their personal information is shared with others. [27]. Privacy is a metric that assesses how well the system safeguards the data of its users [21].

The following mechanisms are used to provide security.

- **Authentication:** Digital certificates are used to authenticate users and the banking system. This authentication method is based on the presence of a Public Key Infrastructure (PKI) and a Certificate Authority (CA), which represents a trusted third-party signing certificate and attests to its validity [23].
- **Non-repudiation:** The usage of the International Mobile Equipment Identity (IMEI) has ensured that no one can deny a transaction [24].
- **Integrity:** The usage of IMEI with elliptic curve cryptography ECC provides mobile users with integrity, non-repudiation, and protection against identity theft, the ECC over binary field is used for key generation, encryption, and decryption to ensure authenticity [24].
- **Confidentiality:** Secure Socket Layer (SSL) provides 128-bit encrypted security so that sensitive information sent over the Internet during online transactions remains confidential [25].

1.2 Usability

The widespread use of mobile phones and the internet has resulted in the development of a variety of applications that provide users with convenient access to services and allow them to perform a variety of tasks at any time. An easy-to-use interface motivates users to use online banking services. The perceived usability of online banking has a big impact on consumers' decisions to use it [5]. To keep their information private and secure, customers should know how to use their online banking accounts appropriately. Because technical terminologies may cause consumers to discard the system immediately, security elements

must be usable and simple in their processes [1]. Usability refers to how simple it is to use a user interface [31]. According to Nielson's Model, usability is determined by five elements. The five attributes mentioned below are commonly used in usability [16]. These attributes are explained as:

1. **Learnability:** Learnability means ease of learning for new users. The availability of guidance (e.g. accessed from the main page), manual, and help features that facilitate learning are important for the learnability attribute [26].
2. **Efficiency:** Efficiency means the high speed of task performance. The inclusion of the main menu on the main page (that can be quickly accessed) is important for efficiency [26].
3. **Memorability:** Memorability means usage over time. This can be achieved through the use of graphics and labeled icons.
4. **Error Prevention:** Error prevention means a low user error rate. Error prevention can be achieved by using a model that is close to the users' mental model.
5. **Satisfaction:** Users' satisfaction. Users' satisfaction can be achieved with high safety and speed of task performance, ease of learning, memorability, and a low error rate.

Different methods can be used to measure usability. Technologies Acceptance Model (TAM) demonstrates how external variables impact people's acceptance of new technology. The usefulness and ease of online banking services have a significant influence on the use of online banking according to the TAM concept. The modified TAM model distinguishes between perceived utility and perceived ease of use [5].

According to the Nielson model, usability is measured on two value scales and is measured as five product attributes: efficiency, learnability, error prevention, memorability, and satisfaction [31].

The Theory of Planned Behavior was used to measure the acceptance of online banking in Tunisia. The Theory of Planned Behavior (TPB) is an extension of the Theory of Reasoned Action and is based on three basic components: attitude, subjective norm, and perceived behavioral control [32].

1.3 Problem Statement

An increase in the use of online banking has been seen, especially during the COVID-19 pandemic, but the general public still hesitates about using it because of its usability and security issues. Several studies show users want usable security and better education. The main issue in the adoption of online banking applications is its difficult interface, the imbalance between security and user experience, and the lack of education about technology.

Security, usability, and user education are the primary concerns in the adoption of online banking. There is a need to identify the issues users face in the security and usability domains while banking online in Pakistan. There is a need to highlight the main reasons for not using online banking applications in Pakistan frequently. Furthermore, there is also a need for user education and users need to be identified in online baking applications. To increase the usage and to provide better, secure, and more convenient functionalities in online banking applications in Pakistan all these issues need to be identified and addressed.

1.4 Purpose of Study

The primary goal of this research work is to investigate the usability and security of online banking applications in Pakistan from the perspective of the end-users. To examine the understanding, acceptance, and awareness of online banking among the general public in Pakistan, this work compares the Pakistani online banking system with the online banking applications in other countries to provide a comparison of their usability and security. This study also explores the level of user education and investigates the view and requirements of online banking applications.

1.5 Research Questions

Question 1: *What is the level of understanding, acceptance, and awareness of online banking in Pakistan?*

Question 2*:* *What reasons prevent or hinder the use of online banking applications in Pakistan?*

Question 3: *What concerns do users have about the usability of online banking applications?*

Question 4: *What concerns do users have about the security of online banking applications?*

Question 5: *How do the security and usability of Pakistani online banking applications compare with international (non-Pakistani) online banking applications?*

Question 6: *Are user's satisfied with the security and usability education/ security and usability-related information provided by online banking services providers?*

Question 7: *What recommendations can (usability and security) experts provide to online banking service providers in Pakistan?*

1.6 Scope

The scope of this thesis is to analyse the security and usability of online banking applications in Pakistan. This study assesses the usability (e.g. do users find it easy to use the interface of a banking application or do users face difficulties? Similarly, it also assesses the security features used by Pakistani banking applications. It also hopes to provide insight into questions such as "How important is convenience or security to the general public?" This work also attempts to determine whether or not users require additional security features e.g. transaction passwords to enhance protection for an online banking transaction. This research highlights the security configurations of systems that handle sensitive online transactions. Additionally, it compares Pakistani online banking applications to international online banking applications to identify gaps and areas of possible improvement.

The result of this work can be used to bring usability and security (e.g. design of interface or inclusion of additional security features) in line with the user's needs and expectations. It will help banks to recognize those features that force users to select weak security measures while using online banking. This work also aims to help online banking service providers make their services more secure, usable, and convenient.

1.7 Limitations of the Study

This research is focused on usable security and as such its goal is limited to the exploration of factors that determine acceptance of online banking. Also, due to time constraints, the scope of this study is limited to a survey and questions on common factors only.

1.8 Advantages and Disadvantages of Online Banking

The main advantage of online banking is convenience. Tasks such as account viewing, bill payment, transaction processing, and financial management are all available through online banking, just as they are in traditional banking. Additionally, online banking provides these services with higher availability (24/7) and lower overhead (e.g. users don't have to wait in lines or go somewhere to conduct their transactions).

There are also some drawbacks to online banking. Examples include:

- Technology issues: users are not familiar with a technology mechanism; they may find it difficult to perform certain tasks.
- Security issues: such as fraud or illegal access to an account through a hacked or stolen password or login information, may result in potential loss.

1.9 Target Group

Academic and professional readers are the intended audience for this study. Additionally, this work can assist banks in better understanding customer needs in terms of online banking acceptance and usage.

1.10 Application

Online banking is a modern subject of study that has attracted a large research community. Online banking is popular because it provides 24/7 availability (regardless of location) and the ability to conduct efficient transactions (without waiting in queues). Usable security for instance a convenient interface that allows users to perform their tasks without any help and efficiently. It also provides protection that makes people feel more secure and confident. As a result, more people are willing to try online banking i.e. a favorable impact on the acceptance of online banking.

CHAPTER 2: LITERATURE REVIEW

This chapter is divided into two main sections. The first section provides the theoretical framework and the second section provides a review of existing literature in this domain.

2.1 Background Concepts

This section presents a description of the basic concepts of online banking.

2.1.1 Online Banking

There are several definitions for online banking, some of which are given below:

- "Online banking enables users to conduct financial transactions over the Internet," [33].
- "Online banking refers to the process of conducting financial transactions over the internet," [6].
- "Online banking aims to deliver banking services via the internet rather than through traditional bank locations," [9].

In the broadest sense, the term "online banking" refers to systems that allow bank customers to access their accounts as well as general information about bank products and services via a

computer or other intelligent device. Many banking transactions can be completed with online banking. An intelligent device could be used to check a bank account, request account transactions, and pay bills electronically. *"The advantage of online banking is that you can pay bills superfast, and your account is automatically created or debited for each deposit and payment, making it easier to stay on track"(SUZE ORMAN)*,[39].

In online banking, the most significant factors are security and usability. "Security refers to a customer's belief that making online payments is secure."[2]. "Usability is how easy it is to use an interface" [22]. Security further depends upon two factors: safety and privacy, while usability depends upon five factors, i.e., learnability, efficiency, memorability, error prevention, and satisfaction.

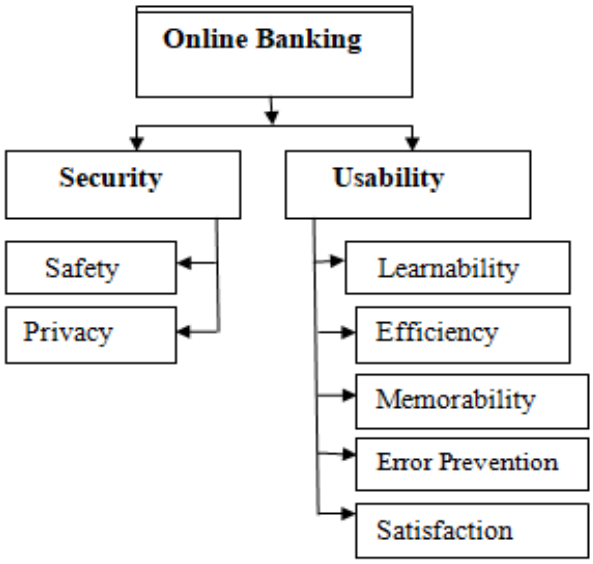


Figure 2.1: Online Banking Model [41]

The purpose of online banking security is to make users feel safe and secure while logging in [1]. Users favor methods that are more ubiquitous and familiar, such as fingerprint

or facial identification, over ones that are slightly less tactile and less understood, such as voice recognition, typing, or gait analysis [7].

2.1.2 Online Banking in Pakistan

Online banking was initially established in Pakistan in the mid-1990s. Only one bank in Pakistan offered online banking services in 2004, and other banks eventually followed suit. Almost all banks now offer online and mobile banking in Pakistan. As a result of COVID-19, the majority of bank account holders in Pakistan, like the rest of the globe, have migrated to online banking and used it to carry out their transactions.

2.1.3 Types of Online Banking

There are various types of online banking, including PC banking, Internet banking, mobile banking, video banking, telebanking, and self-service terminals [40]. Internet banking and mobile banking are the most popular types.

- **Internet Banking:** Internet banking is a service that allows customers to use a bank's official website to access several services. It can be accessed at any time and from any machine using any Web browser.

- **Mobile Banking:** Users may access account information, make payments, get exchange rate information, and much more by using this type of banking. Customers may carry their bank with them wherever they go and conduct critical financial transactions at their fingertips by downloading the bank's online banking application to their smartphones.

2.2 Related Work

Several studies have been conducted on the usability and security of online banking systems in different countries using different techniques.

2.2.1 Review of Studies on Security of Online Banking

A study on online banking security was conducted in Malaysia. In the study Human-computer interaction, usability, and security were all investigated as part of the investigation [1]. An online survey was conducted to examine security issues associated with online banking. There were a total of 137 participants in the study. After the survey, the researchers conducted interviews with 37 people to gain a better understanding of end-user perceptions of online banking in the context of usable security. The findings of this study showed that the majority of consumers struggle to understand technical jargon, as well as the technical elements of warnings and information. To fulfill the usability requirements, there was no user guide accessible. Also, some people were dissatisfied with the current level of security, while others were not sure. Moreover, users were concerned about the security of online banking, this affected their behavior and perception of the service. The results suggest that initiatives to raise end-user awareness should be seriously considered.

A study in Serbia was conducted on information security in internet banking [9]. The researchers reviewed customers' perceptions regarding their needs and familiarity with some of the concepts related to information security. An online survey was conducted to collect data. Statistical analysis and various tests were performed using SPSS. The findings indicated that users were unfamiliar with basic technologies and also identified the key risks associated with Internet banking. This is extremely important for both customers and banks because

customers must understand how to correctly use their internet banking account to keep their information private and secure. According to the findings, users should be aware of the security of their personal information as well as the risks that could damage their privacy and bank accounts when using online banking. Both banks and internet banking customers should work to resolve issues like avoiding online attacks and threats while banking online.

A similar study was conducted to determine the elements that influence users' intentions to continue using online banking in Malaysia [4]. To collect data, researchers used a survey method and managed to obtain 163 participants. The data analysis and hypothesis testing were carried out using the SPSS and the Structural Equation Modeling (AMOS) approach. According to the results, perceived confidentiality, authentications, and data integrity have a positive impact on users' intention to continue using Internet banking in Malaysia. Non-repudiation, on the other hand, was not a significant factor in users' intentions to continue using online banking in Malaysia.

2.2.2 Review of Studies on Usability of Online Banking

A study was conducted, to investigate the elements that influence users' willingness to use online banking in Shandong Province, China [5]. The researchers used the technology acceptance framework for this study. A survey with 52 participants was followed by an interview with 4 participants. According to the findings, *perceived usability* and *perceived credibility* were important characteristics that influenced consumers' intention to use e-banking, while the importance of *perceived ease of use* and *perceived cost* were less important. Furthermore, *difficulty in operation*, *unnecessary use,* and *security concerns* were identified as barriers to the adoption of e-banking. The results suggest that banks should

focus on the most important variable, to maximize potential acceptance. Examples include maximizing strengths and minimizing flaws in e-banking systems and building precise market positioning strategies to align and manage customer expectations.

2.2.3 Review of Studies on Usability and Security of Online Banking

A research study was conducted, to analyse users' opinions on the internet and mobile banking [3]. This study was conducted in Slovenia to learn more about how consumers think about security and how the authentication systems they employ affect user experience. An online survey was conducted among users of fifteen banks in Slovenia to gather data. The results of the survey were analysed and commented on by a small group of banking security specialists who were interviewed as a part of the study. These findings show that Slovenian consumers recognize security as the most important factor in online and mobile banking and that the vast majority of users are aware of available security features. Also, most users believe that additional passwords are essential for security while banking online. Moreover, respondents believe that Internet and mobile banking are useful, that they are generally easy to use, and that learning how to use them is easy. Furthermore, the participants believe that Slovenian banks' security features do not obstruct their use. Results indicate that users of Internet and mobile banking services rate security as the most important feature of these services, although they also demand products that are simple to use.

The research study was conducted on the security and usability of single-factor authentication (SFA) and multifactor authentication (MFA) systems,[2]. In this study security and usability attributes of SFA and MFA were reviewed and addressed. This study involved

a survey with 302 participants (all of whom had at least two international bank accounts). Multi-factor authentication techniques were rated as safe and reliable, with a high usability rating. In terms of usability, both SFA and MFA were considered usable, whereas MFA was considered more secure and trustworthy.

Another similar study was conducted to examine how the general public perceives biometrics in terms of understanding, awareness, and acceptance [7]. A survey of 282 participants was used to gather the general public's views on biometrics. The researchers used thematic analysis and automated word vector analysis on the data to gain a better understanding of the term's perceptions and meaning. The findings show that while most people have a basic awareness of what biometrics is, their knowledge is usually confined to the techniques that they are most familiar with (e.g., fingerprints or facial recognition). Intangible methods (such as typing or gait analysis) are often overlooked or misunderstood. This showed that the public's understanding of these biometric methods should be further improved. Overall, this study provides unique insight into consumers' opinions on biometrics, their understanding of biometric applications, and areas where users may be deficient in knowledge.

A study was performed to analyse the effects of security and usability on electronic banking services [8]. The researchers used survey and regression analytic approaches to conducting their research. According to the findings, security and usability issues with electronic banking services, indicate that with improved security and usability, issues with electronic banking services are reduced.

A study was conducted to identify the most popular online authentication methods used by international banks and compared them to the methods employed by six UAE banks [6].

The researchers also discussed the challenges and attacks that these methods face in terms of authentication. The researchers examined and accessed the authentication mechanisms using two well-defined comparison matrices. One is based on characteristics and the other is based on attack vectors. The results showed that the threat of illegal access can be reduced if the authentication mechanisms utilized are advanced. Advanced authentication mechanisms that are reliable and not vulnerable can ensure that only authorized users have access to the secret information and that they are the only ones who can make the change. Additionally, the findings show that to avoid financial loss and reputation damage due to fraud, identity theft, customer information leakage, data corruption, or unenforceable agreements, an effective authentication system is required.

CHAPTER 3: RESEARCH METHODOLOGY

This chapter presents the thesis workflow: topic selection, theory selection, research procedure, data collection, and analysis methodologies.

3.1 Workflow

The approach used in this thesis is depicted in figure 3.1.

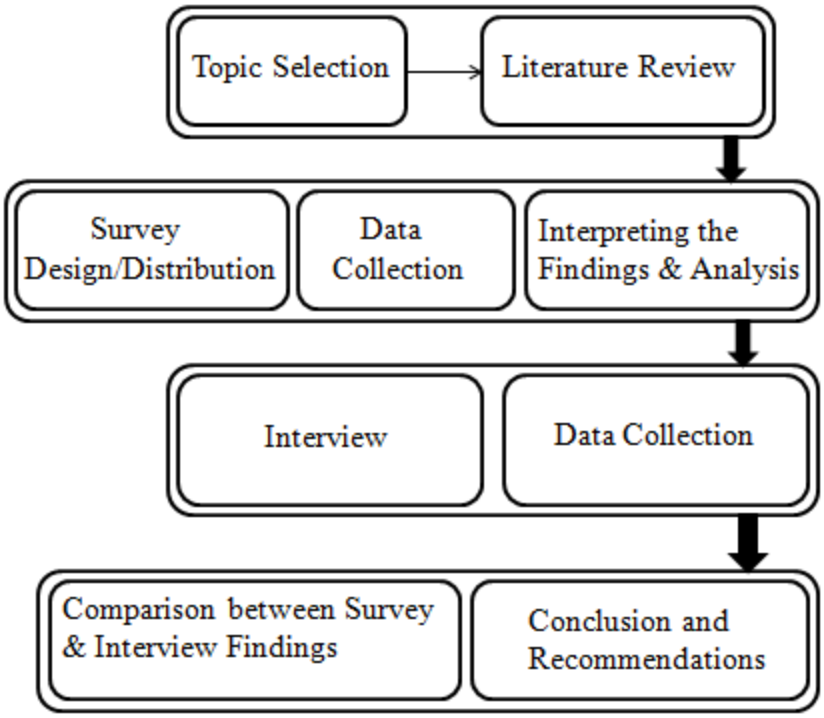


Figure 3.1: Thesis Work Flow

This research started with the selection of the "Analysing the Security and Usability of Online Banking Applications in Pakistan." This was followed by the preparation of relevant

research questions and a review of existing theoretical models. The researcher then discussed major concepts and some existing theoretical models to provide the background for this research. As the structured survey was developed and used to collect primary data. The data from the survey was collected and analysed. A follow-up was then conducted using interview sessions with experts in the domain. Lastly, the conclusions drawn and recommendations made for future work.

3.2 Topic Selection

The Selected topic is pertinent, and vital for the present and future generations. Online banking has been evolving rapidly, especially during the COVID-19 pandemic. Although online banking is gaining popularity, people still hesitate to use it because of its security and usability issues. This topic is also interesting and useful for the banking sector. By providing the answers to questions that are most significant for customers' adoption of online banking in Pakistan, this work can provide significant insight into the security and usability of online banking applications in Pakistan.

There is sufficient literature relevant to the selected topic because usable security is a very important field, particularly in the banking sector.

3.3 Theory Selection

This study has used some established models that have a direct connection with the research questions of this thesis. The theoretical model employed in the thesis is Nielsen's Model. Because of their strong resemblance to the research questions, the Nielsen Model was chosen.

The Nielsen model was chosen because it consists of five important elements: learnability, efficiency, memorability, error prevention, and satisfaction as described in the theoretical framework. These five elements are important for the adoption of technology.

3.4 Research Process

3.4.1 Research Method

In the first step, this study will utilize a survey-based technique to collect primary data. In the next step, this study will interview to obtain expert opinion suggestions for improving the security and usability of online banking applications.

3.4.2 Relationship between Quantitative and Qualitative Approach

This study utilizes both quantitative and qualitative approaches. The relationship between these two is shown in figure 3.2.

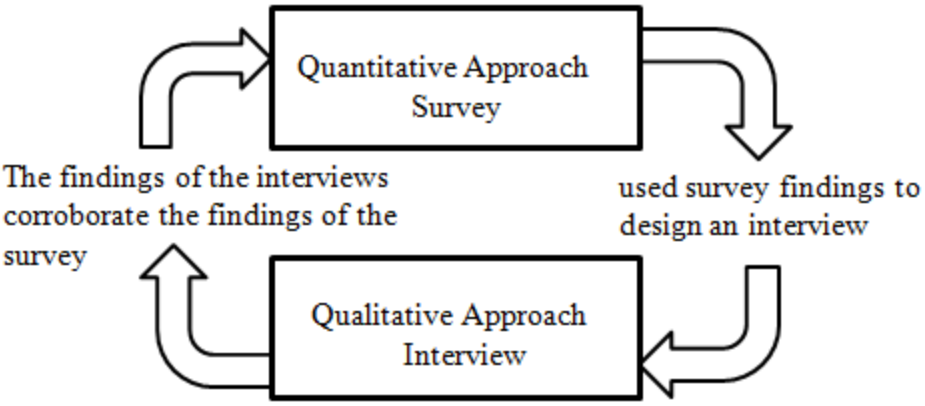


Figure 3.2: Quantitative and Qualitative Approach

3.4.3 Interview Participants Information

An interview session for in-depth insight was conducted regarding the security, usability, and user education in online banking applications. Suggestions for improvements were also requested during the interview. A request was sent to ten experts to participate in the interview session.

Participation in the interview was voluntary, and participants had the open choice of leaving the interview at any stage. A total of eight participants took part in the interview session.

- The first participant is a Post-doc researcher on HCI.
- The 2nd and 3rd participants are online application developers with more than 7 years of experience.
- The 4th and 5th participants are bank employees (in the IT department) with strong background knowledge of Information security (IS).
- The 6th, 7th, and 8th participants have more than 5 years of experience in the information security department.

3.4.4 Quantitative Approach

According to Devin Pickell, a numerical and statistical analysis of statistical and numerical data is quantitative research (numbers and statistics) [35].

In the first phase of this study, a quantitative approach is used. A questionnaire-based survey is developed and distributed. Then the data is collected and numerical and statistical analysis is carried out.

3.4.4.1 Design of Survey for Users

All the research questions listed in section 1.5 were used to design the questions in the survey. The survey design is based on commonly reported and underlying factors.

Table 3.1: Design of Survey

Sections	Contents
1	Demographic information and users/non-users ratio
2	Reasons for not using online banking
3	Awareness among users
4	Usability analysis
5	Usability analysis sub-section (manual/help features)
6	Usability analysis sub-section (efficiency, memorability, error prevention, and satisfaction)
7	Security and education analysis
8	The ratio of international online banking users participating in the survey.
9	Usability comparison with international online banking.
10	Guidance/help feature comparison with international online banking.
11	Remaining usability factor analysis comparison with international online banking.
12	Security and education analysis comparison with international online banking.

3.4.4.2 Sampling Technique

The designed survey was distributed among Pakistani nationals. The channels used for the distribution of the survey were online: email and social media. Convenience sampling was used meaning the online survey link was emailed to friends, family members, and university students (with the request to forward the link to their friends and acquaintances). Social media, including Facebook, WhatsApp, and LinkedIn was also used to distribute the survey.

3.4.4.3 Data Collection

Data can be gathered in a variety of ways. Interviews, surveys, panels, focus groups, participant observation, documentation, and databases are the most frequent data collection methods. This study will use primary data based on questionnaires and interviews. From the online survey distribution, a total of 302 responses were collected. Three responses were deleted after thorough consideration of all responses, and 299 were used for analysis purposes.

3.4.4.4 Data Analysis

The data collected by the survey will be analysed using the Statistical Package for the Social Sciences (SPSS), version 22.

3.4.4.5 Interpretation of Findings

The results of the survey will be presented in the form of tables.

3.4.5 Qualitative Approach

In the second phase of this study, a qualitative approach involving non-numerical data that is open-ended (concept, descriptions, meanings, words, and more) will be used to collect data via interviews.

3.4.5.1 Design of Interview for Experts

Research questions number 3, 4, 5, 6, and 7 (listed in section 1.5) were used to design the questions in the interview. The structure of the interview is shown in table 3.2.

Table 3.2: Design of Interview

Sections	Contents
1	Participant's experience in UX/UI/HCI or IS
2	Questions related to usability analysis.
3	Questions related to security analysis.
4	Questions related to usability and security analysis.
5	Questions related to user education.
6	Questions related to comparison.
7	Question on recommendation, suggestions.

3.4.5.2 Sampling Technique

Ten experts were contacted to participate in this study. Eight participants consented to be interviewed. The channel used for the interview was online via Zoom. The interview questions were sent to all the participants one day in advance, so they could deliberate and prepare adequate answers.

3.4.5.3 Data Collection

In the second phase of this study, qualitative data will collect through an interview session.

3.4.5.4 Data Analysis

In the second phase of this study, the data collected through interviews will be analysed manually by the researcher.

3.4.5.5 Interpretation of Findings

In this phase, non-statistical data collected through interviews will be presented in the form of tables.

3.4.6 Primary Data

According to Fisher, primary data gathering is a phase in which the researcher discovers information through investigation rather than from existing literature [38]. Therefore, to fulfill the research goal, this study employs survey and interview research methods, in which primary data is obtained by questionnaire and interview.

3.4.6.1 Survey and Interview Methods

To analyse awareness and acceptance of online banking applications by the general public as well as security and usability issues in online banking applications, it is important to understand the users' experiences and opinions on online banking applications. Therefore a questionnaire was created to collect data. For an in-depth understanding of the survey findings, an interview session was held to collect data.

3.4.6.2 Questionnaire/Interview Methodology

Structured and unstructured questionnaires are the two types of questionnaires. Structured questionnaires consist of closed-end-type questions, while unstructured questionnaires contain open-ended-type questions. Structured questionnaires are used for quantitative investigations and have fixed options such as multiple-choice, yes/no, or true/false questions. Unstructured questionnaires consist of open-ended questions in which respondents are not limited to a single response option [37].

If a researcher wishes to quantify the study material and compare the perspectives and experiences of different users, Fisher suggests that they employ a structured questionnaire approach [38]. The questionnaire-based survey used in this research utilizes a structured and unstructured approach. On the other hand, the interview session utilizes an unstructured approach to obtain the perspectives and experiences of experts and compare them to the users' perspectives.

3.4.6.3 Survey Format

The survey should have a logical and sequential structure that allows the respondent to understand what the survey is about, and it should be concise [38]. The designed survey consists of 12 short sections.

There are a variety of survey styles available, including dichotomous, MCQs, Checklists, Rating Scales, and Ranking Questions. In this survey, multiple-choice questions and rating scales were used for the structured questions. Multiple choice questions offer several possibilities from which the responder must choose the most appropriate or correct answer. For the rating scale questions, a rating scale is used, ranging from “strongly agree” to “strongly disagree”. As some questions are unstructured in this survey, white spaces (adequate for a short paragraph) were provided for responses.

3.5 The research’s validity and reliability

The author focused on peer-reviewed journal and conference articles to ensure the research's validity and reliability. The papers were found in Springer Link, IEEE, Google Scholar, ACM Digital Library, and Science Direct databases. All the chosen publications are from the online databases of the National University of Science and Technology.

The following actions were taken to ensure the research's validity:

- The questionnaire-based survey was designed based on existing research, theory, and models in the domain of acceptance of online banking applications.
- 302 responses were collected, out of which 299 responses were found to be complete and relevant.

- Following the survey results were used to obtain insight and compared to responses given by experts during the interview sessions.

CHAPTER 4: RESULTS AND ANALYSIS

This chapter presents the data analysis of the survey and interview.

4.1 Survey

The online survey was distributed through email and social media. The author requested family members, relatives, colleagues, friends, and friends of friends to participate in the survey and to further distribute survey links among Pakistani nationals. The author satisfies the audience by mentioning that all efforts will be made to protect participant identity; email addresses will not be collected, and all collected data will be used solely for educational purposes. Participation in the survey study was strictly voluntary, and participants could refuse to participate at any stage. The author received responses from the general public that way.

4.1.1 Demographic Information

This section presents demographic information (e.g. gender, age, education) of the respondents.

Gender

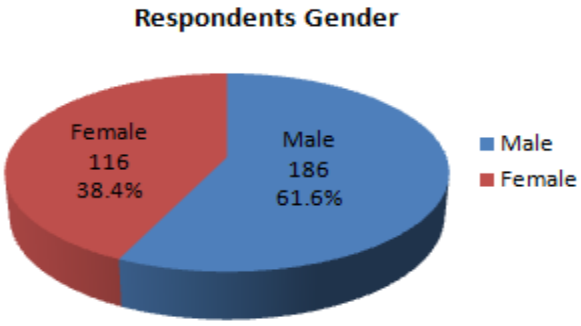


Figure 4.1: Respondents' Gender

302 people actively participated in the survey, of which 186 (61.6%) were males and 116 (38.4%) were females.

Age

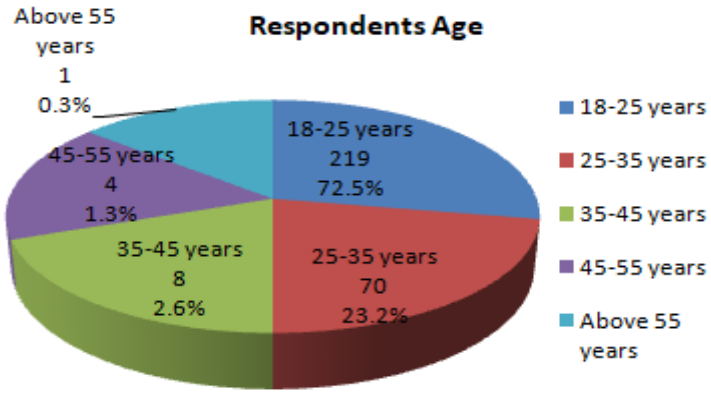


Figure 4.2: Respondents' Age

The result of the survey showed that: 219 (72.5%) respondents were from the 18-25 year age group; 70 (23.2%) respondents were from the 25-35 year age group; 8 (2.6%) respondents were from the 35-45 year age group; 4 (1.3%) respondents were from the 45-55 year age group, and 1 (0.3%) respondent was above the 55-year age group.

Education

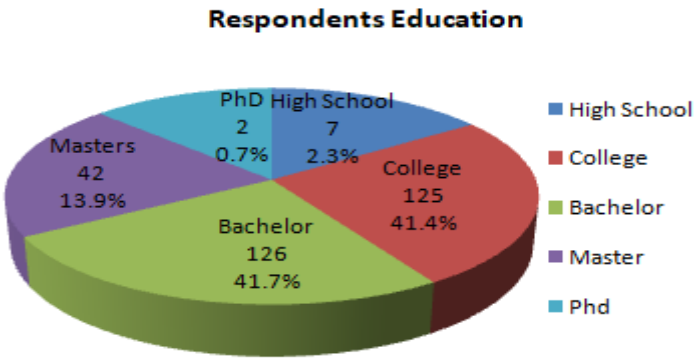


Figure 4.3: Respondents' Education

The results show that: 126 respondents were bachelor's degree holders, 42 were master's degree holders, 125 were college graduates, 7 were high school graduates, and 2 were PhDs.

Computer Expertise

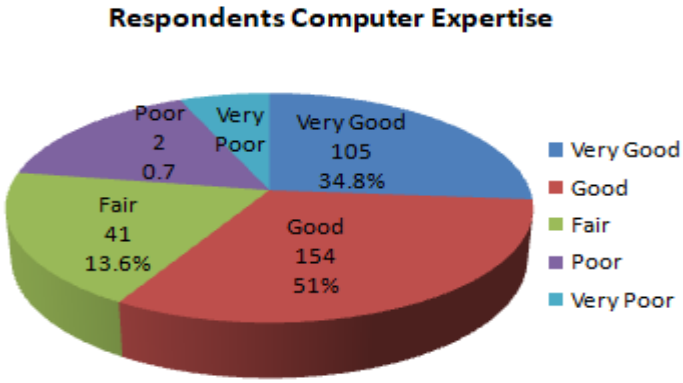


Figure 4.4: Respondent's Computer Expertise

The computer expertise of respondents was measured using a five-step Likert scale. The results show that 105 respondents' computer expertise was very good, 158 respondents' computer expertises were good, 41 respondents' computer expertises were fair and 2 respondents' computer skills were poor.

Security Expertise

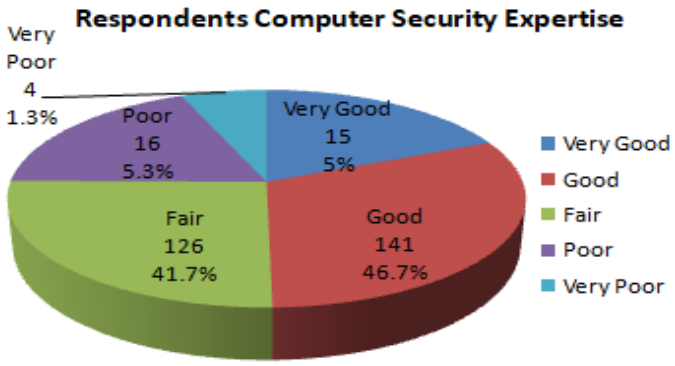


Figure 4.5: Respondent's Computer Security Expertise

The computer security expertise of respondents was measured using a five-step Likert scale. The results show that 15 respondents' computer security expertise was very good, 141 respondents' computer security expertise was good, 126 respondents' computer security expertise was fair, 16 respondents' computer security expertise was poor and 4 respondents' computer security expertise was very poor.

Nationality

Figure 4.6: Respondents' Nationality

The results show that all the respondents were Pakistani nationals.

4.1.2 Users and Non-Users

Question: *Do you use online banking?*

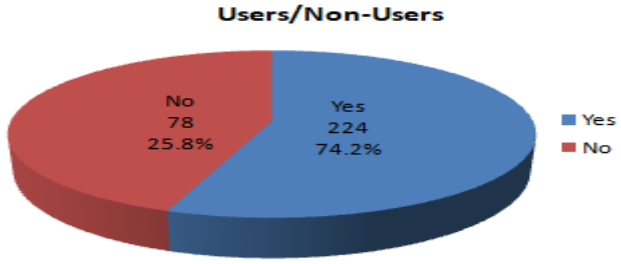


Figure 4.7: Users and Non-Users

Figure 4.7 shows that out of 302 respondents, 224 (74.2%) were online banking application users, while 78 (25.8%) were non-users.

Hypothesis 1 (a)

There will be a difference between the ratio of users and non-users of online banking applications.

Table 4.1: Hypothesis 1(a)

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
User/Non Users	302	1.2583	.43841	.02523

One-Sample Test

	Test Value = 151					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
User/Non Users	-5935.560	301	.000	-149.74172	-149.7914	-149.6921

The results in Table 4.8 indicate:

- The t-static value in the one-sample test is -5935.560
- The degree of freedom, df, is 301

- The significance level, a p-value of the one simple test is 0.000, which is also written as p < .001

Interpretation of the results: The one-sample standard test has a significance level of alpha= 0.05. The p-value from the above results is < .001 which is less than the significance level. As it is less than alpha, we can conclude that there is a difference between the ratio of users and non-users of online banking applications. Hence, hypothesis **H1 (a)** holds.

4.1.3 Reasons for not using online banking

Question: *What are your main reasons for not using online banking?*

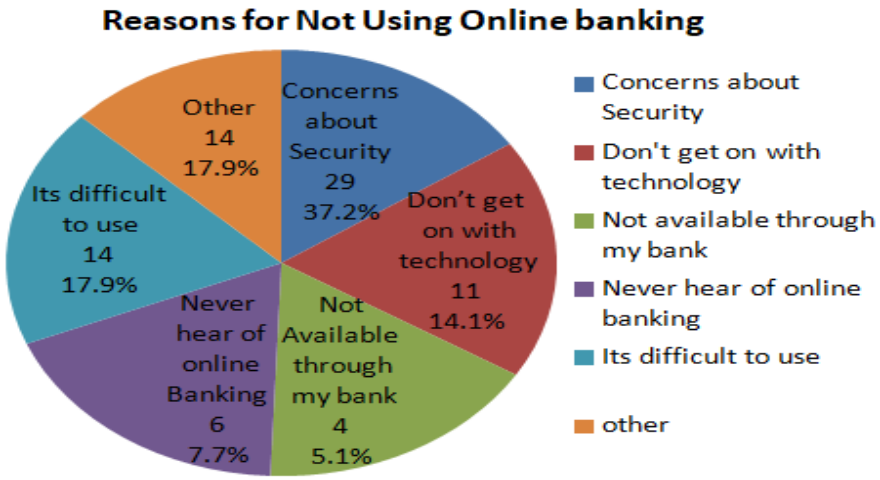


Figure 4.8: Reasons for Not Using Online Banking

Results show that out of 78 non-user respondents, 29 (37.2%) respondents were concerned about security, while 11 (14.1%) respondents said that, they shouldn't get on with technology. 4 (5.1%) respondents said that online banking application services are not available through their bank, 6 (7.7%) respondents said that they had never heard of online banking, 14 (17.9%) respondents said that they were not using online banking because it's

difficult to use (usability issues), and 14 (17.9%) respondents described other reasons for not using online banking applications.

Hypothesis 1 (b)

Those who do not use online banking do so, generally, to avoid security and usability issues,

Table 4.2: Hypothesis 1 (b)

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
Reasons for not using online banking	78	3.0897	2.02058	.22879

One-Sample Test

	Test Value = 13					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Reasons for not using online banking	-43.317	77	.000	-9.91026	-10.3658	-9.4547

These results indicate that:

- The t static value in the one-sample test is -43.317
- The degree of freedom, df, is 77
- The significance level, a p-value of the one-simple test is 0.000, which is also written as p < .001

Interpretation of the results: The significance level of the one-sample test is alpha=0.05. The p-value from the above result is < .001 which is less than the significance level. As it is less than alpha, we can conclude that Hypothesis **H1 (b)** holds.

4.1.4 General Information

Online banking Services Providers

Question: *In Pakistan, which bank do you use for most of your online banking services?*

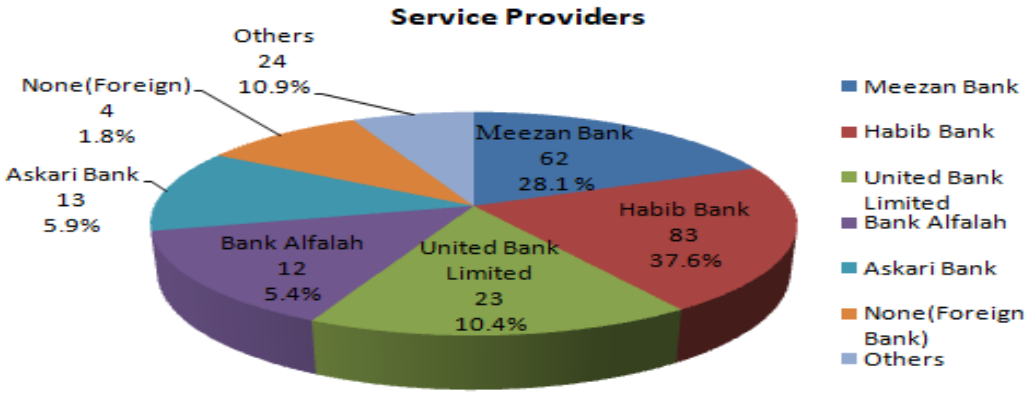


Figure 4.9: Service Providers

The top five online banking service providers in Pakistan were included.

Figure 4.9 shows that 62 (28.1%) respondents were Meezan Bank online banking services users, 83 (37.6%) respondents were Habib Bank online banking services users, 23 (10.4%) respondents were United Bank limited online banking services users, 12 (5.4%) respondents were Bank Alfalah online banking services users, 13 (5.9) respondents were Askari Bank online banking services users, 4 (1.8%) respondents were foreign online banking application users, and 24 (10.9%) respondents were other banks' online banking services users.

Frequency of using online banking applications

Question: *How often do you use online banking?*

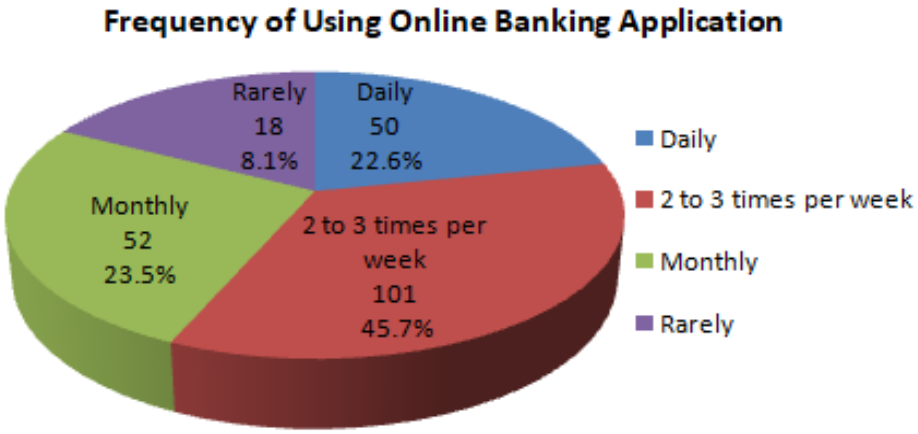


Figure 4.10: Frequency of Using Online Banking Applications

Figure 4.10 shows that 50 (22.6%) respondents were using online banking applications daily, 101 (45.7%) respondents were using online banking applications two to three times per week, 52 (23.5%) respondents were using online banking applications monthly, and 18 (8.1%) respondents were using online banking applications rarely.

Online Banking Applications

Question: *Which online banking application do you commonly use?*

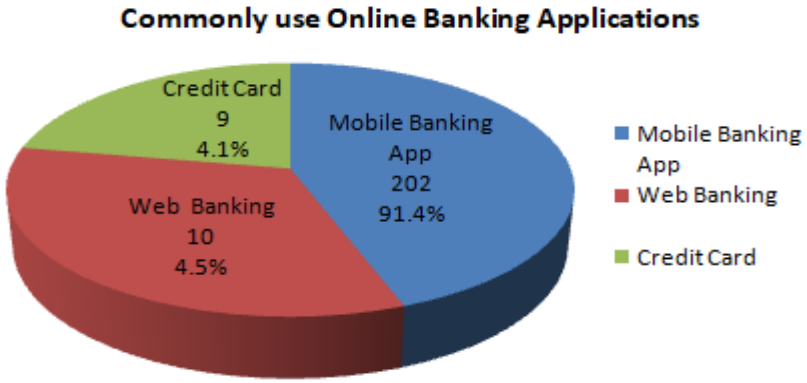


Figure 4.11: Commonly Use Applications

Figure 4.11 shows that 202 (91.4%) respondents were using a mobile banking app, 10 (4.5%) respondents were using a web banking application, and 9 (4.1%) respondents were using a credit card banking application.

Control over Online Banking

Question: *Do you think that using online banking is entirely within your control?*

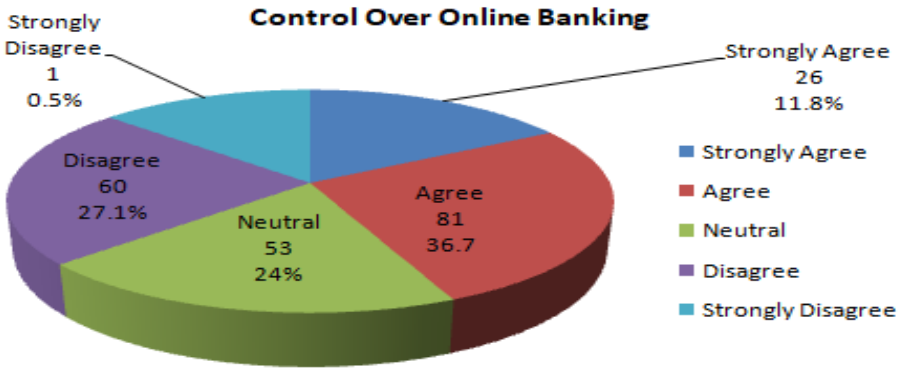


Figure 4.12: Control over Online Banking

Respondents' control over online banking applications was measured on a five-step Likert scale. Figure 4.12 shows that 26 (11.8%) respondents strongly agreed, 81 (36.7%) respondents agreed, 53 (24.0%) respondents were neutral, 60 (27.1%) respondents disagreed, and 1 (0.5%) respondent was strongly disagreed.

4.1.5 Usability Analysis

This section is about usability analysis based on the five factors stated in Nielson's model.

Learnability

Question: *Do you know how to find informative guidelines, manuals, or how to use help features while using online banking applications?*

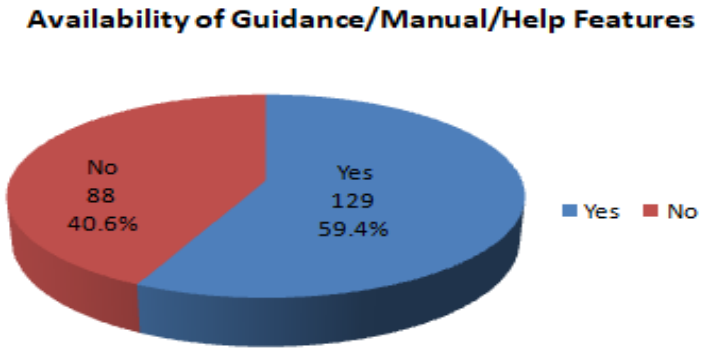


Figure 4.13: Availability of Guidance /Manual/ Help Features

Figure 4.13 shows that 129 (59.4%) respondents were knowledgeable about help features, while 88 (40.6%) respondents were not aware of help features.

Question: *Do you find manual/guidance/help features useful?*

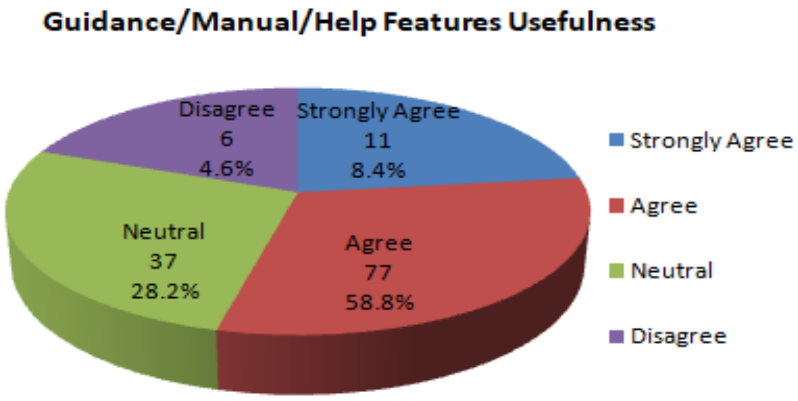


Figure 4.14: Guidance/Help Features Usefulness

The author further placed a question for those who know about help features, to understand how much help features are useful. A five-step Likert scale was used to measure the usefulness of help features. Figure 4.14 shows that 11 (8.4%) respondents strongly agree, 77 (58.8%) respondents agree with help features' usefulness, 37 (28.2%) respondents are neutral, and 6 (4.6%) respondents disagree with help features' usefulness.

Efficiency

Question: *Do you know all the features/functions provided in online banking applications?*

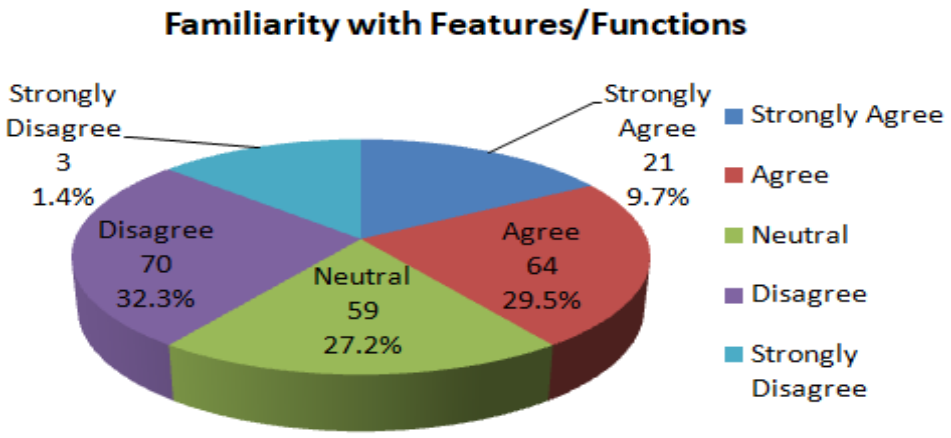


Figure 4.15: Familiarity with Features / Functions

Results showed that 21 (9.7%) respondents strongly agreed that they knew all features and functions provided in online banking applications, 64 (29.5%) respondents agreed that they knew all the features and functions of online banking applications, 59 (27.2%) respondents were neutral, 70 (32.3%) respondents disagreed and 3(1.4%) respondent strongly disagreed that they knew all the features and functions of online banking applications.

Hypothesis 2(a)

There will be a greater number of users who are not familiar with all functions/features provided in online banking.

Table 4.3: Hypothesis 2 (a)

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
Familiar with all features/functions	217	2.8618	1.02255	.06942

One-Sample Test

	Test Value = 43.4					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
Familiar with all features/functions	-583.995	216	.000	-40.53825	-40.6751	-40.4014

The results indicate that:

- The t static value in the one-sample test is -583.995
- The degree of freedom, df, is 216
- The significance level, a p-value of the one-sample test is 0.000, which is also written as p < .001

Interpretation of the results: The significance level of the one-sample test is alpha=0.05. The p-value from the above results is < .001 which is less than the significance level. As the p-value it is less than alpha, hence, hypothesis **H2 (a)** holds and we can conclude that there are a greater number of users who are not familiar with all the features provided in online banking.

Question: *Do you face any difficulties and/or problems when using online banking applications (e.g. unable to login, transfer money, etc.)?*

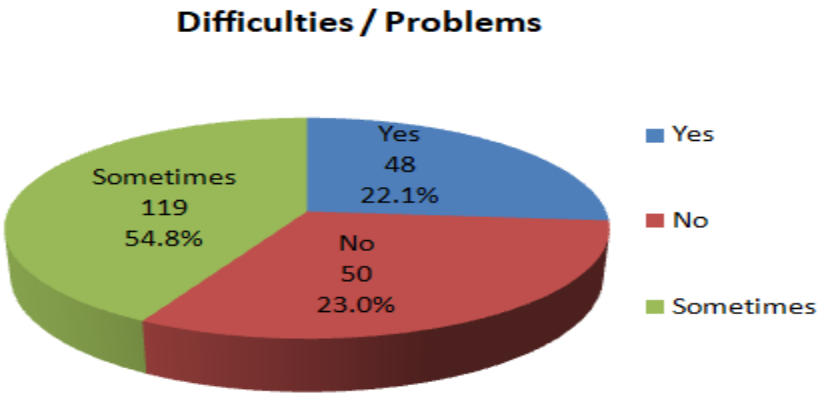


Figure 4.16: Difficulties / Problems

Figure 4.16 shows that 48 (22.1%) respondents were facing difficulties and problems while using online banking applications, 50 (23.0%) respondents were not facing any difficulties or problems and 119 (54.8%) respondents were facing difficulties sometimes while banking online.

Memorability

Question: *Does your online banking application use graphics and helpful label icons for the convenience of customers using the application after a long time?*

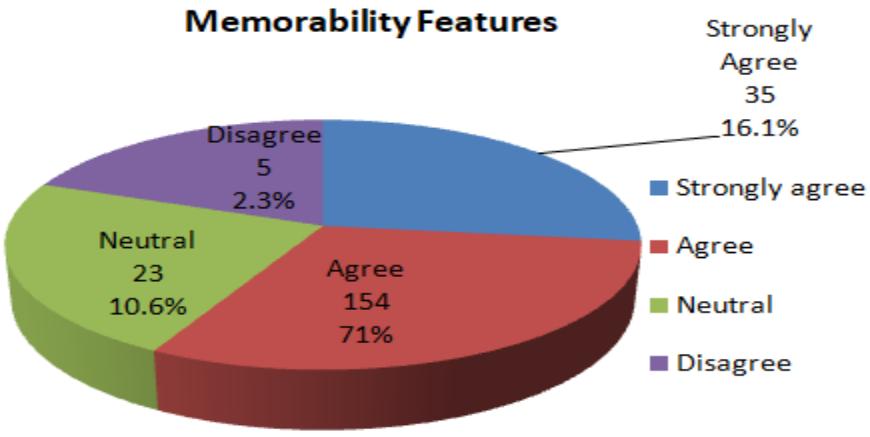


Figure 4.17: Memorability Features

Figure 4.17 shows that 35 (16.1%) respondents strongly agree with the question statement, 154 (71%) respondents agreed, 23 (10.6%) respondents are neutral, and 5 (2.3%) respondents disagree with the question statement.

Error Prevention

Question: *If you wanted to report a security breach or ask a question about the security of an online banking application, where would you do this (e.g. block/unblock debit card)?*

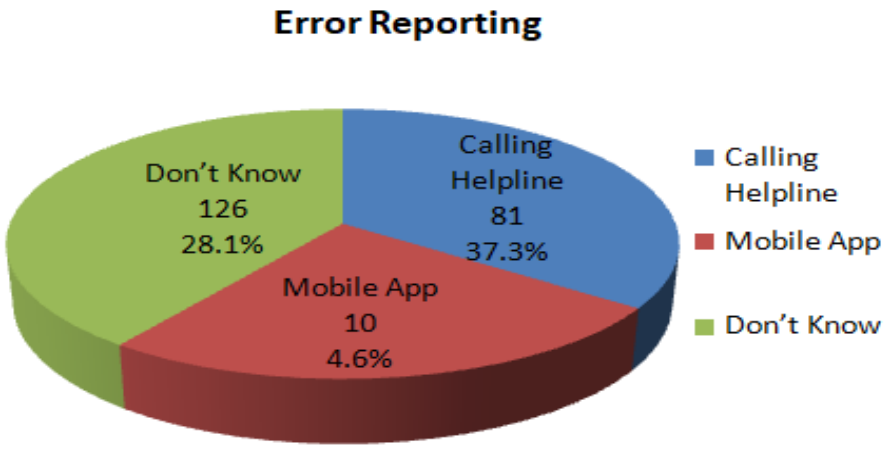


Figure 4.18: Error Reporting Features

The result shows that 81 (37.3%) respondents said that they will call the helpline, 10 (4.6%) respondents said that they will use a mobile app for this purpose, while 126 (58.1%) respondents said that they don't know where to report an error or incident.

Hypothesis 2(b)

There will be a greater number of users who are unaware of where to report in case of an error/incident while banking online.

Table 4.4: Hypothesis 2 (b)

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
Incident report	217	2.2074	.95662	.06494

One-Sample Test

	Test Value = 72.3					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Incident report	-1079.346	216	.000	-70.09263	-70.2206	-69.9646

The results indicate that:

- The t static value in the one-sample test is -1079.346
- The degree of freedom, df, is 216
- The significance level, a p-value of the test is 0.000, which is also written as $p < .001$

Interpretation of the results: The significance level of the one-sample test is alpha= 0.05. The p-value from the above result is < .001 which is less than the significance level. As the p-value is less than alpha, hence, hypothesis **H2 (b)** holds and we can conclude that there are a greater number of users who are unaware of where to report in case of error/incident while banking online.

Satisfaction

Question: *Do you think online banking applications in Pakistan are complicated for non-technical users?*

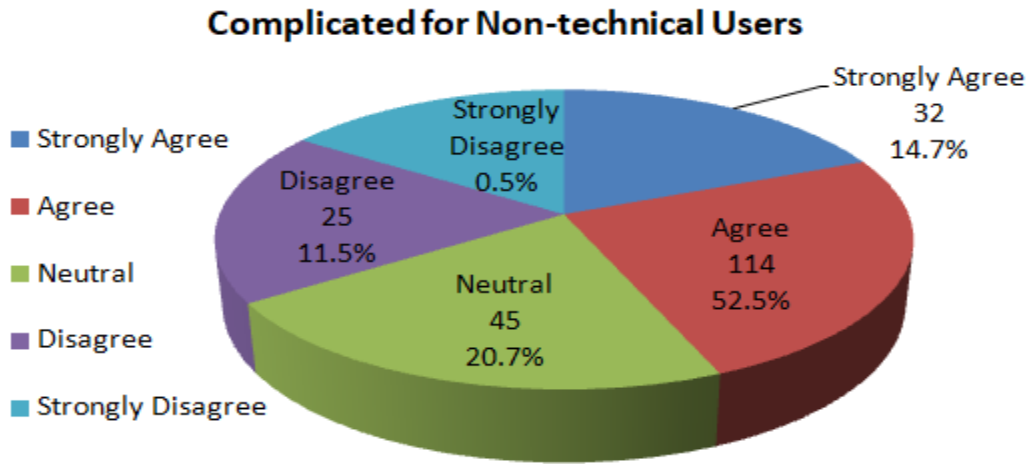


Figure 4.19: Complicated for Non-technical Users

Figure 4.19 shows that 32 (14.7%) respondents strongly agreed, 114 (52.5%) respondents agreed, 45 (20.7%) respondents were neutral, 25 (11.5%) respondents disagreed while 1 (0.5%) respondents strongly disagreed with the question statement that online banking applications in Pakistan are complicated for non-technical users.

Question: *Do you think that the authentication features limit you when you use online banking applications?*

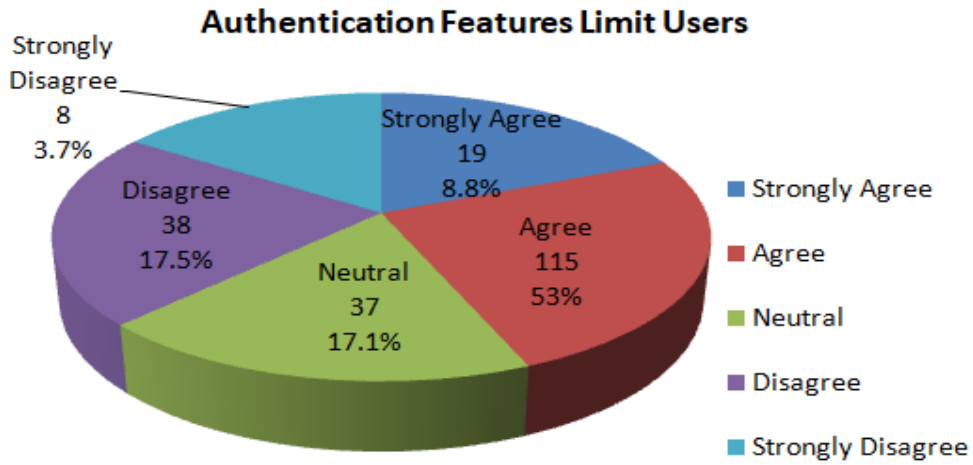


Figure 4.20: Authentication Features Limit Users

Results show that 19 (8.8%) respondents strongly agree that the authentication features limit users while banking online, 115 (53%) respondents agree with the question statement, 37 (17.1%) respondents are neutral, 38 (17.5%) respondents disagree, and 8 (3.7%) respondents strongly disagree with the question statement.

Hypothesis 2(c)

There will be a majority of users who want those authentication features that don't limit users while banking online.

Table 4.5: Hypothesis 2 (c)

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
Authentication Features limit users	217	2.5438	.99962	.06786

One-Sample Test

	Test Value = 43.4					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Authentication Features limit users	-602.081	216	.000	-40.85622	-40.9900	-40.7225

The results indicate that:

- The t static value in the one-sample test is -205.904
- The degree of freedom, df, is 104
- The significance level, a p-value of the test is 0.000, which is also written as $p < .001$

Interpretation of the results: The significance level of the one-sample test is alpha= 0.05. The p-value from the above result is < .001 which is less than the significance level. As the p-value is less than alpha, hence, hypothesis **H2(c)** holds and we can conclude that there are a majority of users who want those authentication features that don't limit users while banking online.

4.1.6 Security Analysis

This section is about the security analysis of online banking applications in Pakistan.

Question: *Do you know the correct web address of your bank?*

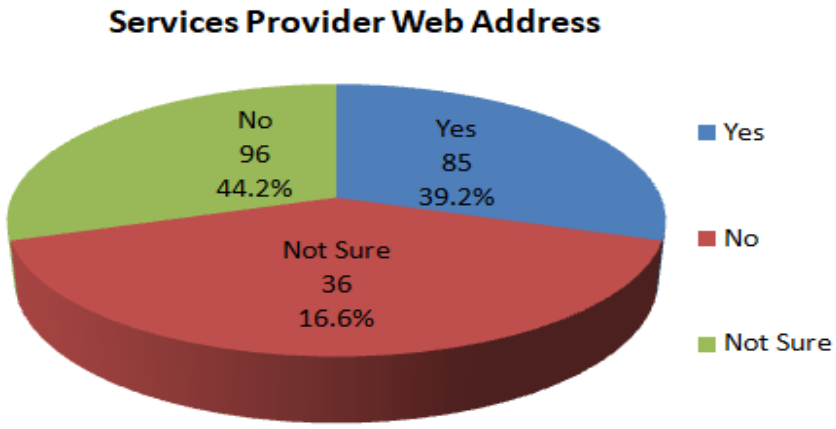


Figure 4.21: Service Provider Web Address

Figure 4.21 shows that 85 (39.2%) respondents said "Yes" that they know the correct web address of their bank; 96 (44.2%) respondents said "No" they don't know the correct web address of their bank, and 36 (16.6%) respondents were not sure about the correct web address of their bank.

Question: *In Pakistan, which authentication mechanism(s) does your bank mostly use for online banking applications?*

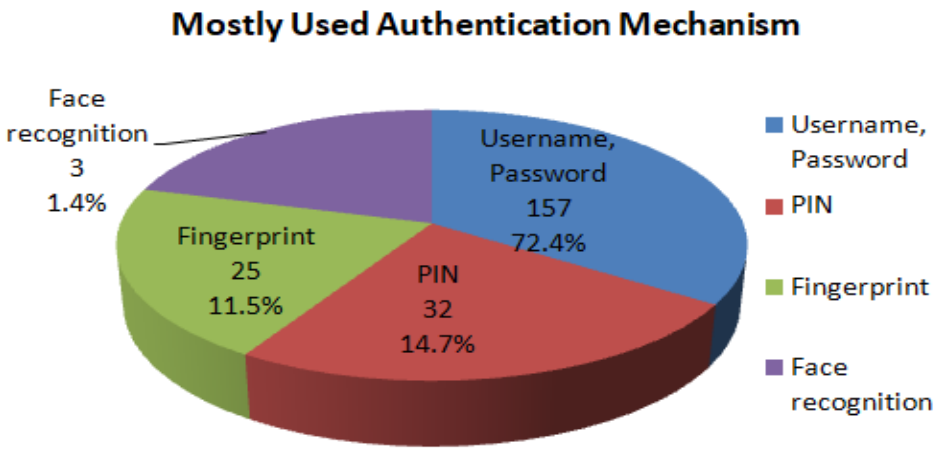


Figure 4.22: Mostly Used Authentication Mechanism

Figure 4.22 shows that 157 (72.4%) of the respondents said that their bank mostly used usernames and passwords as an authentication mechanism. According to 32 (14.7%) respondents, their bank mostly used PIN as an authentication mechanism, 25 (8.3%) respondents said that their bank used fingerprint as an authentication mechanism, while 3 respondents said that their bank used face recognition as authentication in online banking applications.

Question: *Do you use the same password for different online banking applications?*

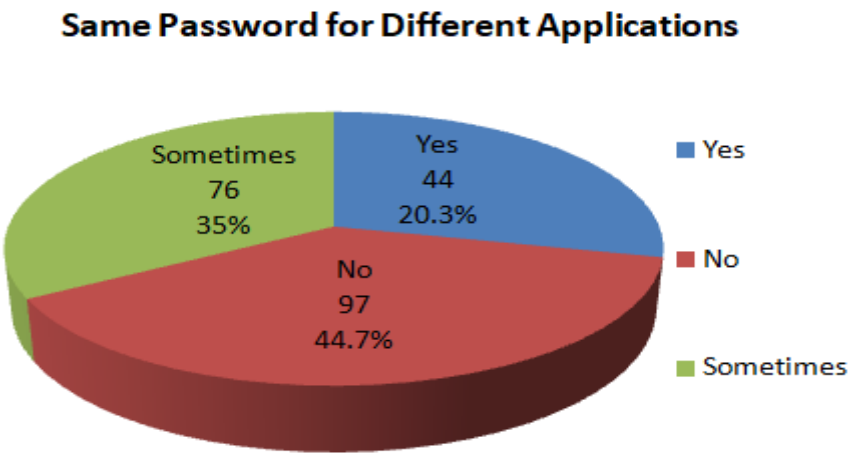


Figure 4.23: Same Password for Different Applications

Figure 4.23 shows that 44 (20.3%) respondents were using the same password for different applications, 97 (44.7%) respondents were not using the same password for different applications, and 76 (35%) respondents were sometimes using the same password for different online banking applications.

Question: *Does your bank verify your password for each online banking application separately (instead of allowing you to use the same password for all its online banking applications)?*

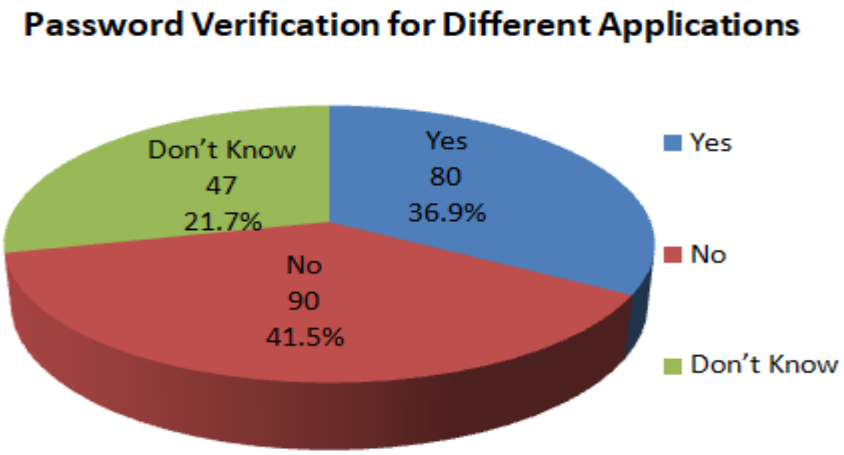


Figure 4.24: Password Verification for Different Applications

Figure 4.24 shows that 80 (36.9%) respondents said yes, their bank verifies users' passwords separately for each online banking application. 90 (41.5%) respondents said no, their bank does not verify passwords separately for different online banking applications, while 47 (21.7%) respondents didn't know that their bank verifies passwords for each online banking application separately.

Question: *Does your online banking application require additional authentication at the time of the transaction (e.g. image-based password, security question, one-time password, transaction password, etc.)?*

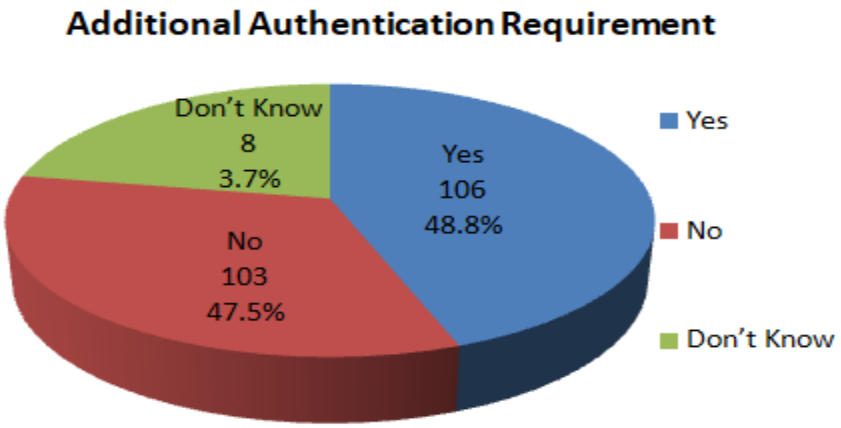


Figure 4.25: Additional Authentication Requirement

Figure 4.25 shows that 106 (48.8%) respondents said yes, their online banking applications require additional authentication at the time of transaction. 103 (47.5%) respondents said no, their online banking applications don't require additional authentication at the time of the transaction, while 8 (2.6%) respondents said that they don't know whether their online banking applications require additional authentication at the time of transaction or not.

Question: *Do you think that additional authentication is needed (e.g. during transactions)?*

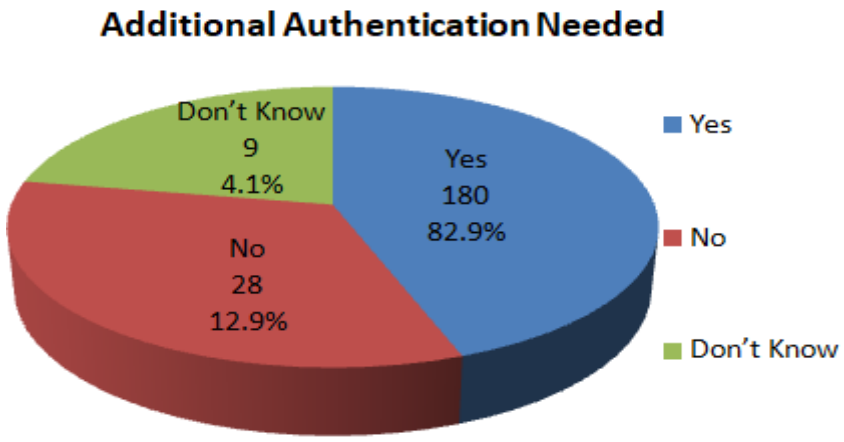


Figure 4.26: Additional Authentication Needed

Figure 4.26 shows that 180 (82.9%) respondents said yes, additional authentication is needed during transactions, 28 (12.9%) respondents said no, additional authentication is not needed during transactions, and 9 (4.1%) respondents said they "don't know" whether additional authentication is needed during transactions or not.

Hypothesis 3 (a)

There will be a greater number of users who will prefer additional authentication at the time of transaction.

Table 4.6: Hypothesis 3 (a)

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
Additional Authentication Needed	217	1.2120	.50115	.03402

One-Sample Test

	Test Value = 43.4					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Additional Authentication Needed	-1240.083	216	.000	-42.18802	-42.2551	-42.1210

The results indicate that:

- The t static value in the one-sample test is -1240.083
- The degree of freedom, df, is 216
- The significance level, a p-value of the test is 0.000, which is also written as $p < .001$

Interpretation of the results: The significance level of the one-sample test is alpha= 0.05. The p-value from the above result is < .001 which is less than the significance level. As the p-value is less than alpha, hence, hypothesis **H3 (a)** holds and we can conclude that there are a greater number of users who prefer additional authentication at the time of transaction.

User Education/Awareness

Question: *Does your bank provide its customers with security-related information/guidelines? (e.g., regular update of software, use of strong passwords)*

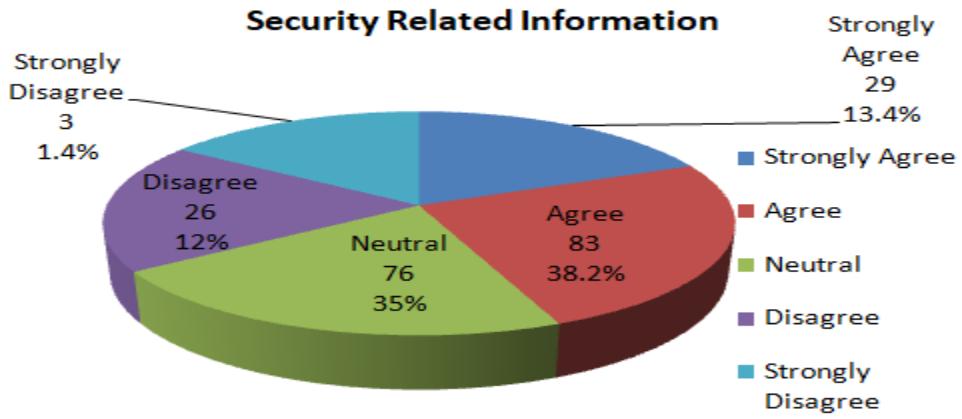


Figure 4.27: Security-Related Information

Figure 4.27 shows that 29 (13.4%) respondents strongly agree that their bank provides security-related information, 83 (38.2%) respondents agree that their bank provides security-related information, 76 (35%) respondents are neutral about the question statement, 26 (12%) respondents disagree with the question statement, and 3 (1.4%) respondent strongly disagrees with the question statement.

Question: *Do you know the various security features used by your online banking applications (e.g. digital certificate, HTTPS, lock icon, etc.)?*

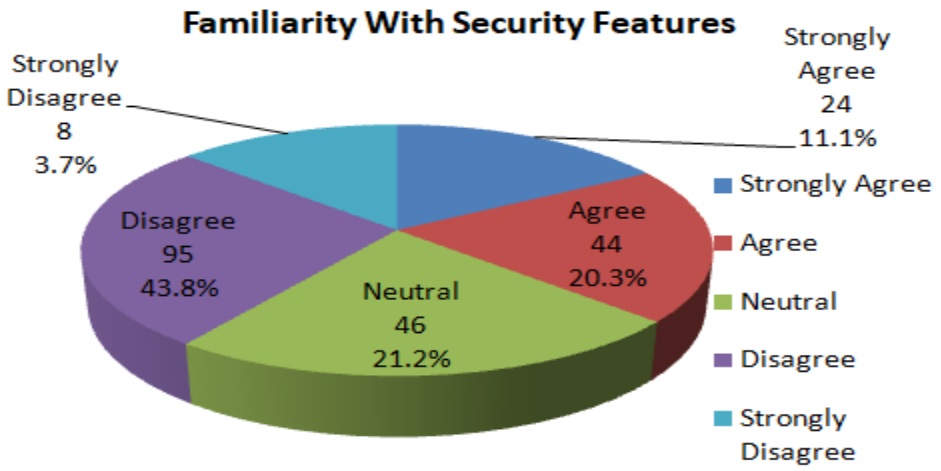


Figure 4.28: Familiarity with Security Features

Figure 4.28 shows that 24 (11.1%) respondents strongly agreed that they know the various security features used by their online banking applications, 44 (20.3%) respondents agreed with the question statement, 46 (21.2%) respondents were neutral about the question statement, 95 (43.8%) respondents disagreed, that they know the various security features used by their online banking applications, and 8 (3.7%) respondents strongly disagreed with the question statement.

Hypothesis 3(b)

There will be a greater number of users who will not be familiar with most of the security features used by online banking applications.

Table 4.7: Hypothesis 3 (b)

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
Familiar with Security Features	217	3.0876	1.10834	.07524

One-Sample Test

	Test Value = 43.4					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Familiar with Security Features	-535.793	216	.000	-40.31244	-40.4607	-40.1641

The results indicate that:

- The t static value in the one-sample test is -535.793
- The degree of freedom, df, is 216
- The significance level, a p-value of the test is 0.000, which is also written as $p < .001$

Interpretation of the results: The significance level of the one-sample test is alpha= 0.05. The p-value from the above result is < .001 which is less than the significance level. As the p-value is less than alpha, hence, hypothesis **H3(b)** holds and we can conclude that there are a greater number of users who are not familiar with most of the security features used by online banking applications.

Question: *Do you think convenience or security is more important for you when using banking online applications?*

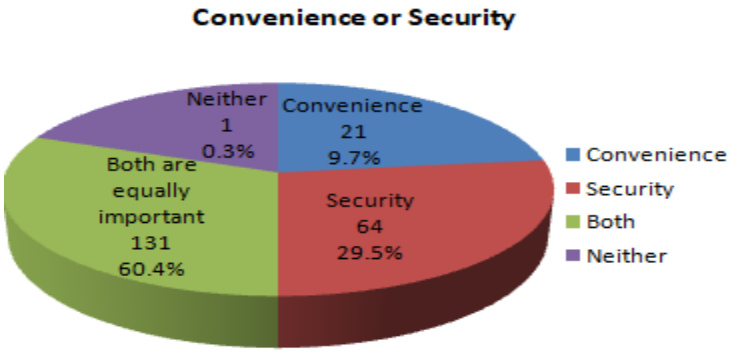


Figure 4.29: Convenience or Security

Figure 4.29 shows that 21 (9.7%) respondents said that convenience is more important while banking online, 64 (29.5%) respondents said that security is more important while banking online and 131 (60.4%) respondents said that "both are equally important", while 1 (0.5%) respondent said neither security nor convenience is important.

Hypothesis 3(c)

There will be a greater number of users who will prefer convenience and security while banking online.

Table 4.8: Hypothesis 3 (c)

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
Convience or Security	217	2.5161	.67424	.04577

One-Sample Test

	Test Value = 54.25					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Convience or Security	-1130.291	216	.000	-51.73387	-51.8241	-51.6437

The results indicate that:

- The t static value in the one-sample test is -1130.291
- The degree of freedom, df, is 216
- The significance level, a p-value of the test is 0.000, which is also written as $p < .001$

Interpretation of the results: The significance level of the one-sample test is alpha= 0.05. The p-value from the above result is < .001 which is less than the significance level. As the p-value is less than alpha, hence, **hypothesis H3(c)** holds and we can conclude that there are a greater number of users who prefer convenience and security while banking online.

Question: *How concerned are you about the security of online banking? Keep in mind that "security" means privacy, confidentiality, and proof of identity.*

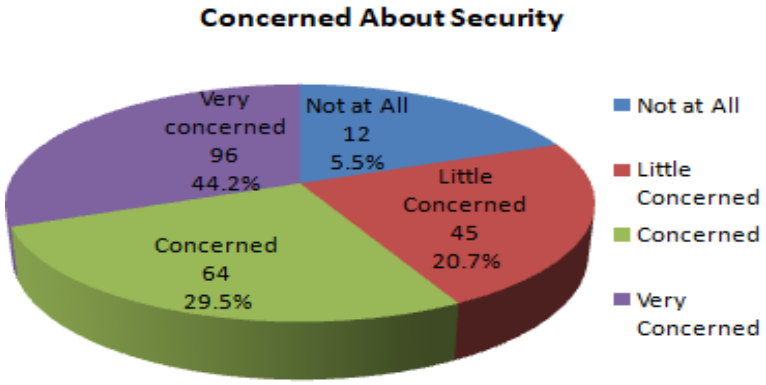


Figure 4.30: Concerned About the security

Figure 4.30 shows that 12 (5.5%) respondents were not at all concerned about the security of online banking, 45 (20.7%) respondents were a little concerned about the security of online banking, 64 (21.2%) respondents were concerned about the security of online banking, and 96 (31.8.2%) respondents were very concerned about the security of online banking.

Question: *Which security measures are best for securing you against various kinds of online banking attacks? Select all that apply.*

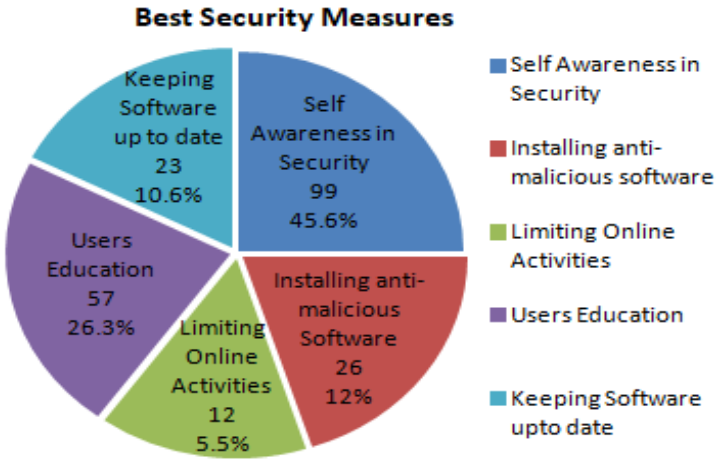


Figure 4.31: Best Security Measures

Figure 4.31 shows that 99 (45.6%) respondents said that self-awareness in security, 26 (12%) respondents said that installing anti-malicious software, 12 (5.5%) respondents said limiting online activities, 57 (26.3%) respondents said users' education, and 23 (7.6%) respondents said keeping software up-to-date are the best security measures for securing users against various kinds of online attacks.

Question: *Which authentication features do you think are not necessary for securing your online banking applications? Select all that apply.*

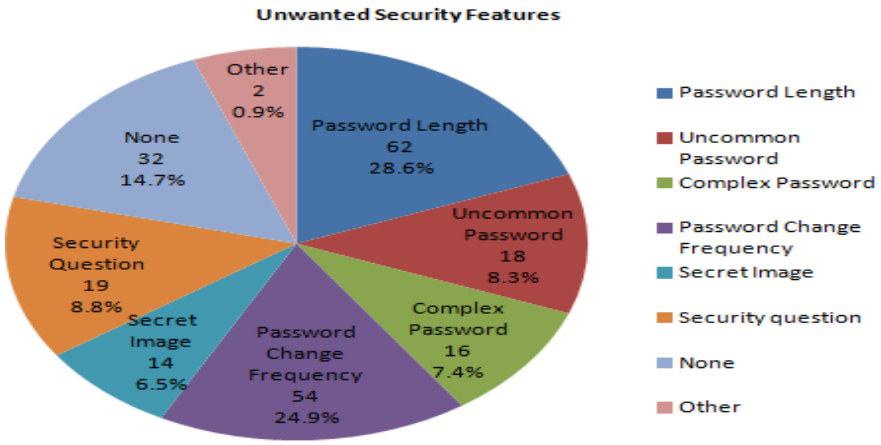


Figure 4.32: Unwanted Security Features

Figure 4.32 shows that 62 (28.6%) respondents said that password length is not necessary, 18 (8.3%) respondents said that uncommon passwords are not necessary, 16 (5.3%) respondents said that complex passwords are not necessary, 54 (24.9%) respondents said that password change frequency is an unwanted feature, 14 (6.5%) respondents said that secret image is not necessary, 19 (8.8) respondents said that security questions are an unwanted feature, and 32 (14.7%) respondents said that none of the authentication features are unwanted features in online banking applications.

Question: *Do you feel secure sending sensitive information during online banking applications?*

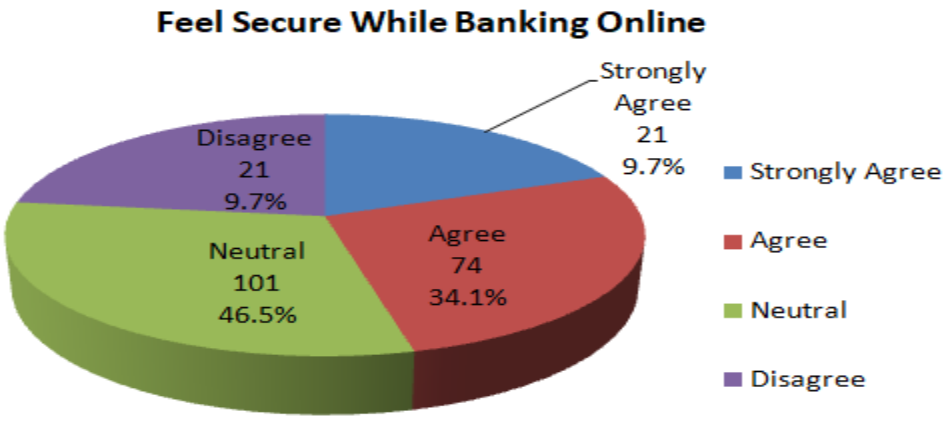


Figure 4.33: Feel Secure While Banking Online

Figure 4.33 shows that 21 (9.7%) of respondents said that they strongly agree with the question statement, 74 (34.1%) respondents said that they agree with the statement, 101 (46.5%) respondents said that they are neutral with the statement, and 21 (9.7%) respondents disagreed with the question statement.

Question: *Are you satisfied with the security features currently provided by the online banking applications you use?*

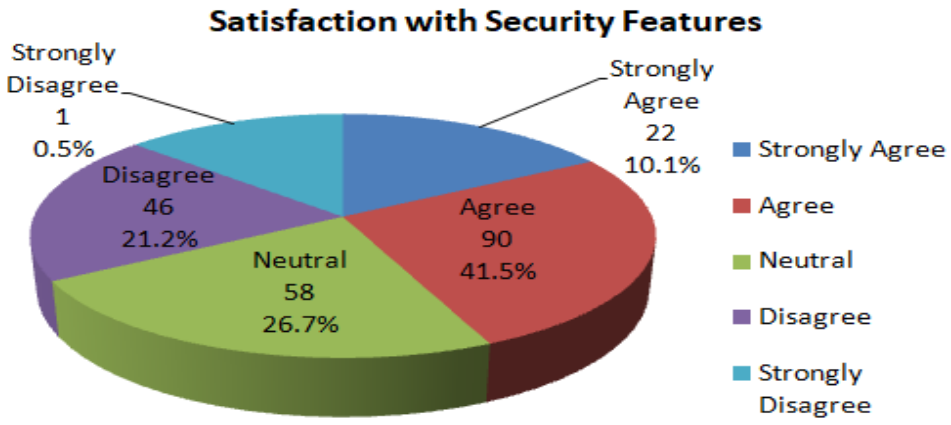


Figure 4.34: Satisfaction with Security Features

Figure 4.34 shows that 22 (10.1%) respondents were said that they strongly agree with the security features provided in online banking applications, 90 (41.5%) respondents said that they agree with the question statement, 58 (26.7%) respondents were neutral with the statement, and 46 (21.2%) respondents said that they disagree with the question statement, while 1 (0.5%) respondent strongly disagreed with the security features currently provided in online banking applications.

Question: *Are advanced authentication methods used in your online banking applications? (Note: Simple authentication methods include passwords while advanced authentication methods include iris scan and facial recognition.)*

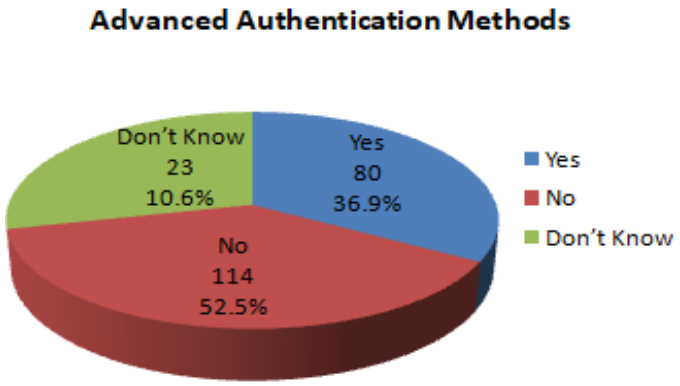


Figure 4.35: Advanced Authentication Methods

Figure 4.35 shows that 80 (36.9%) respondents said yes their online banking applications use advanced authentication methods, 114 (52.5%) respondents said no their online banking applications do not use advanced authentication methods, and 23 (10.6%) respondents said they don't know whether their online applications use advanced authentication methods like iris scan, face recognition, fingerprints, etc.

4.1.7 Comparison with International Online Banking

This section compares the security and usability of online banking applications in Pakistan with international online banking applications.

This section repeated the same questions for international online banking applications as used for Pakistani online banking applications.

This section further consists of two subsections; the first subsection is about the usability analysis of online banking applications, while the second subsection is about the security analysis of online banking applications. Only 15 responses were collected from the participants who had experience with both Pakistani as well as international online banking applications.

Question: *Are you using any foreign bank account for online banking?*

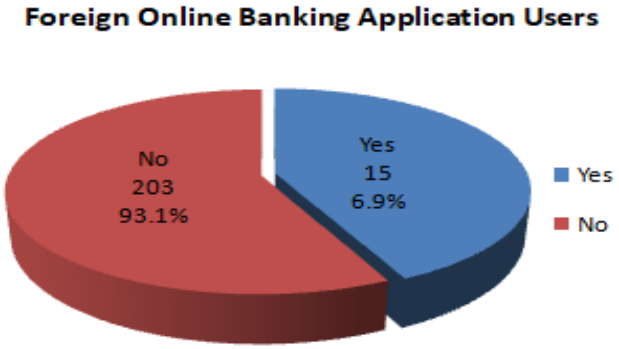


Figure 4.36: Foreign Online Banking Application Users

Figure 4.36 shows that 15 (6.9%) respondents were foreign online banking application users, while 203 (93.1%) respondents said that they were not using any foreign online banking applications.

Question: *Which foreign online bank do you use for online banking applications (e.g. National Bank of Dubai, United Arab Emirates)?*

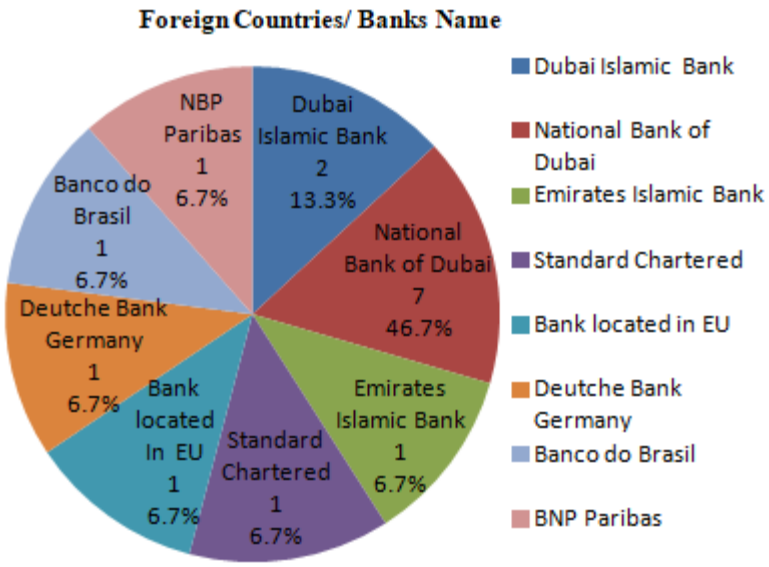


Figure 4.37: Foreign Countries/ Banks Name

Figure 4.37 shows that 2 (13.3%) respondents were using Dubai Islamic Bank (UAE) online banking services, 7 (46.7%) respondents were using National Bank of Dubai (UAE) online banking services, 1 (6.7%) respondent was using Emirates Islamic Bank(UAE) online banking services, 1 (6.7%) respondent was using Standard Chartered online banking services, 1 (6.7%) respondent was using online banking services of the bank located in EU, 1 (6.7%) respondent was using Deutsche Bank (Germany) online banking services, 1 (6.7%) respondent was using bank Banco do Brasil (Brazil) online banking services and 1 respondent was using BNP Paribas (France) online banking services.

Usability Analysis of International Online Banking Applications

The results on usability obtained from the limited users who used international online banking applications are shown in Table 4.9.

Table 4.9: Usability Analysis of International Online Banking Applications

Learnability	How to find help features/manual	Yes 14	No 1			
	Help features/ manual useful	Strongly Agree 3	Agree 11	Neutral 1	Disagree 0	Strongly Disagree 0
Efficiency	User face difficulties/ Problems	No 13	Sometime 2	Yes 0		
	Familiar with OB features/functions	Strongly Agree 3	Agree 10	Neutral 2	Disagree 0	Strongly Disagree 0
Memorability	Use of helpful graphic/ label icons	Strongly Agree 6	Agree 8	Neutral 1	Disagree 0	Strongly Disagree 0
Error Prevention	Incident Report	By Calling Helpline 7	Through Mobile App 1	Through Web Option 1	Visit Bank Branch 1	Don't Know 5
Satisfaction	The use of the application is complicated for non-technical users	Strongly Agree 2	Agree 2	Neutral 4	Disagree 6	Strongly Disagree 1
	Authentication features limit users	Strongly Agree 2	Agree 6	Neutral 3	Disagree 4	Strongly Disagree 0

Table 4.9 shows that:

- **Learnability:** The result shows that 14 respondents knew how to find manual help features while banking online. 3 respondents strongly agreed, 10 respondents agreed with the usefulness of help features, guidance, and manual, while 1 respondent was neutral.
- **Efficiency:** The result shows that two respondents stated that they occasionally encounter difficulties or problems when banking online.10 respondents agreed, 3 strongly agreed with the question statement, that they know all the features provided in online banking applications, while 2 respondents were neutral with the question statement.
- **Memorability:** The result shows that 8 respondents agreed, 6 respondents strongly agreed, while 1 respondent was neutral with the statement that their online banking applications provide memorability features.
- **Error prevention:** In case of error or incident report, 7 respondents said they will prevent errors by calling the helpline, 1 respondent said that they will use a mobile app for this purpose, 1 respondent said that they will use the web option, and 1 respondent said they will visit a bank branch, while 5 respondent said that they don't know where they will have to report in case of error or incident.
- **Satisfaction:** The result shows that 2 participants strongly agreed, 2 participants agreed, 4 participants were neutral, and 6 participants disagreed with the statement that the use of applications is complicated for non-technical users.

  The results showed that 2 respondents strongly agreed, 6 respondents agreed, 3 respondents were neutral, and 4 respondents disagreed with the statement that the authentication features limit users.

Security Analysis of International Online Banking Applications

Table 4.10 presents the results of the security analysis of international online banking applications.

Table 4.10: Security Analysis of International Online Banking Applications

Do you know the correct web address	Yes 7	No 6	Not Sure 2		
Mostly Use Authentication Mechanism	Username/ Password 8	PIN 5	Image-based Password 0	Fingerprint 1	Face recognition 1
Use of the same password for different applications	Yes 2	No 5	Sometimes 8		
	Yes	No	Don't Know		
Verify the password for each application separately	10	3	2		
Require additional authentication at the time of transactions	12	3	0		
Additional Authentication is needed	10	4	1		
Use of Advanced Authentication Methods	10	5	0		

Table 4.10 shows that:

- **Do you know the correct web address of your foreign bank?**

  The results show that 7 respondents said yes, they know the web address of their bank, 6 respondents said no, and 2 respondents said they are not sure about the correct web address of their online banking services provider.

- **Which authentication mechanism(s) does your foreign bank mostly use for online banking applications?**

  The results show that 8 respondents said that username and password were the most commonly used authentication mechanisms. 5 respondents said PIN, 1 respondent said fingerprint, and 1 respondent said that face recognition was most commonly used as an authentication mechanism.

- **Do you use the same password for different online banking applications?**

  The results show that two respondents said they use the same password for different applications; five said no, and eight said they occasionally use the same password for different online banking applications.

- **Does your foreign bank verify your password for each online banking application separately (instead of allowing you to use the same password for all its online banking applications)?**

  The results show that 10 respondents said yes to the statement, 3 respondents said no, while 2 respondents said they didn't know about the statement that their bank “verifies the password for each online application separately”.

- **Does your foreign online banking application require additional authentication at the time of the transaction (e.g. image-based password, security question, one-time password, transaction password, etc.)?**

  The results show that 12 respondents said yes, their online banking application requires additional authentication, while 3 respondents said no, their online banking application does not require additional authentication at the time of transaction.

- **Do you think that additional authentication is needed (e.g. during transactions) in foreign online banking applications?**

  The results show that 10 respondents said yes, additional authentication is needed during transactions, 4 respondents said no, additional authentication is not needed during transactions, while 1 respondent said I don't know if additional authentication is needed during transactions.

- **Are advanced authentication methods used in your foreign online banking applications? (Note: Simple authentication methods include passwords while advanced authentication methods include iris scan and facial recognition.)**

  The results show that 10 respondents said that their online banking application uses advanced authentication mechanisms, while 5 respondents said that their online banking application does not use advanced authentication mechanisms like face recognition or fingerprints.

User Education Analysis of International Online Banking Applications

Table 4.11 presents the results of user education analysis of international online banking applications.

Table 4.11: User Education Analysis of International Online Banking Applications

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Do you know various security features provided by foreign OB services provider	2	9	4	0	0
Security-related information provided by Foreign OB services provider	7	7	1	0	0
Foreign OB applications are convenient in use as compared to Pakistan	4	7	2	2	0
Feel secure while banking online	4	9	2	0	0
Online Account creation	Yes 12	No 3	0	0	0

Table 4.11 shows that:

- **Do you know the various security features used by your foreign online banking applications (e.g. digital certificate, HTTPS, lock icon, etc.)?**

  The results show that 2 respondents strongly agreed, 9 respondents agreed, while 4 respondents were neutral with the question and stated that they know of various security features provided by foreign online banking applications.

- **Does your foreign bank provide its customers with security-related information/guidelines? (e.g., regular update of software, use of strong passwords)**

  The results show that respondents strongly agreed, 7 respondents agreed, while 1 respondent was neutral with the question statement that their bank provides its customers with security-related information.

- **Do you think that your foreign online banking applications are convenient to use as compared to Pakistan's online banking applications?**

  The results show that 4 respondents strongly agreed, 7 respondents agreed, 2 respondents were neutral, and 2 respondents disagreed with the statement that foreign online banking applications are more convenient in use as compared to Pakistani online banking applications.

- **Does your foreign bank allow you to create an account without physically visiting the bank (online account creation)?**

  The results show that 12 respondents said yes while 3 respondents said no about the statement: that their foreign banks allow creating an online account.

- **Do you feel secure while sending sensitive information during foreign online Banking?**

  The results show that 4 respondents strongly agreed, 9 respondents agreed, and 2 respondents were neutral with the statement that they feel secure while sending sensitive information during international online banking.

Hypothesis 4 (a, b)

There will be differences between Pakistani and International online banking (security and usability domain).

Hypothesis 4 (a)

Usability:

Table 4.12: Hypothesis 4 (a)

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference Lower	Upper			
Pair 1	Difficulties/Problem - Difficulties/Problems in foreign online banking	.15385	.80064	.22206	-.32998	.63767	.693	12	.502
Pair 2	Guidence/Manual,help features - Manual/Guidence/Help features in foreign online banking	.30769	.63043	.17485	-.07327	.68865	1.760	12	.104
Pair 3	Help features useful - In foreign online banking Manual/Help features useful	.37500	.51755	.18298	-.05768	.80768	2.049	7	.080
Pair 4	Familiar with all features/functions - Familiar with Foreign online banking Features	.92308	1.03775	.28782	.29597	1.55018	3.207	12	.008
Pair 5	Use of Graphic/lable icons - Use of graphics/lable icon in Foreign Online banking	.07692	.49355	.13689	-.22133	.37517	.562	12	.584
Pair 6	Incident report - In foreign Online Banking report of incident	.69231	1.10940	.30769	.02190	1.36271	2.250	12	.044
Pair 7	Complicated for non-technical - Foreign Online Banking is complicated for no technical users	-.92308	1.25576	.34828	-1.68192	-.16423	-2.650	12	.021

These results indicate that:

Pair 1:

- The t-static value is 0.693
- The degree of freedom, df, is 12
- The significance level, a p-value of the paired sample test is 0.502

Pair 2:

- The t-static value is 1.76
- The degree of freedom, df, is 12
- The significance level, a p-value of the paired sample test is 0.104

Pair 3:

- The t-static value is 2.049
- The degree of freedom, df, is 7
- The significance level, a p-value of the paired sample test is 0.80

Pair 4:

- The t-static value is 3.207
- The degree of freedom, df, is 12
- The significance level, a p-value of the paired sample test is 0.008

Pair 5:

- The t-static value is 0.562
- The degree of freedom, df, is 12
- The significance level, a p-value of the paired sample test is 0.584

Pair 6:

- The t-static value is 2.250
- The degree of freedom, df, is 12
- The significance level, a p-value of the paired sample test is 0.044

Pair 7:

- The t-static value is -2.650
- The degree of freedom, df, is 12
- The significance level, a p-value of the paired sample test is 0.021

Interpretation of the results: The significance level of the paired sample test is alpha = 0.05. The p-values from the above results are 0.502, 0.104, 0.80, 0.008, 0.584, 0.044, and 0.021 which are greater than the significance level. As p-values are greater than alpha, hence, hypothesis **H4 (a)** does not hold and we can conclude that there is no significant difference between the Pakistani and international online banking in the usability domain.

Hypothesis 4 (b)

Security:

Table 4.13: Hypothesis 4 (b)

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference Lower	Upper			
Pair 1	Web Address - Web address of Foreign bank	-.07692	.49355	.13689	-.37517	.22133	-.562	12	.584
Pair 2	Security information - Security related information provided in foreign online banking applications	.30769	.94733	.26274	-.26477	.88016	1.171	12	.264
Pair 3	Familiar with Security Features - Familiar with security features used by foreign online banking	.46154	.96742	.26831	-.12307	1.04614	1.720	12	.111
Pair 4	Additional Authentication Needed - Additional Authentication needed in foreign online banking application	-.30769	.75107	.20831	-.76156	.14617	-1.477	12	.165
Pair 5	Satisfied with Security Features - satisfied with the security features provied by foreign online banking	.30769	1.65250	.45832	-.69091	1.30629	.671	12	.515
Pair 6	Use of Advanced Authentications - Use of Advanced Authentication in foreign online banking	.23077	.92681	.25705	-.32930	.79083	.898	12	.387

These results indicate that:

Pair 1

- The t-static value is -0.562
- The degree of freedom, df, is 12
- The significance level, the p-value of the paired sample test is 0.58.

Pair 2

- The t-static value is 1.171
- The degree of freedom, df, is 12
- The significance level, the p-value of the paired sample test is 0.264

Pair 3

- The t-static value is 1.72
- The degree of freedom, df, is 12
- The significance level, the p-value of the paired sample test is 0.111

Pair 4

- The t-static value is -1.477
- The degree of freedom, df, is 12
- The significance level, the p-value of the paired sample test is 0.165

Pair 5

- The t-static value is 0.671
- The degree of freedom, df, is 12
- The significance level, the p-value of the paired sample test is 0.515

Pair 6

- The t-static value is 0.898
- The degree of freedom, df, is 12
- The significance level, the p-value of the paired sample test is 0.387

Interpretation of the results: The significance level of the paired sample test is alpha = 0.05. The p-values from the above results are 0.584, 0.264, 0.111, 0.165, 0.515, and 0.387, which are greater than the significance level. As p-values are greater than alpha, hence, hypothesis **H4 (b)** does not hold and we can conclude that there is no significant difference between the Pakistani and international online banking in the security domain.

4.2 Summary of Hypothesis Testing

Table 4.14 summarizes all the hypotheses other than the usability-related hypothesis and security-related hypothesis and shows whether they were valid or not.

Table 4.1: Hypothesis Summary

Hypothesis	Supported	Not-supported
H1 (a): There will be a difference between the ratio of users and non-users of online banking applications.	✓	
H1 (b): Those who do not use online banking do so, generally, to avoid security and usability issues.	✓	
H4 (a): There will be differences between Pakistani and International online banking (usability domain).		**X**
H4 (b): There will be differences between Pakistani and International online banking (security domain).		**X**

4.3 Summary of Usability-related Hypothesis

Table 4.15 summarises the entire usability-related hypothesis and shows whether they were valid or not.

Table 4.1: Summary of Usability-related Hypothesis

Hypothesis	Supported	Not - Supported
H2 (a): There will be a greater number of users who are not familiar with all functions/features provided in online banking.	✓	
H2 (b): There will be a greater number of users who are unaware of where to report in case of an error/incident while banking online.	✓	
H2 (c): There will be a majority of users who want those authentication features that don't limit users while banking online.	✓	

4.4 Summary of Security-related Hypothesis

Table 4.16 summarises the entire security-related hypothesis and shows whether they were valid or not.

Table 4.1: Summary of Security-related Hypothesis

Hypothesis	Supported	Not-Supported
H3 (a): There will be a greater number of users who will prefer additional authentication at the time of transaction.	✓	
H3 (b): There will be a greater number of users who will not be familiar with most of the security features used by online banking applications.	✓	
H3 (c): There will be a greater number of users who will prefer convenience and security while banking online.	✓	

4.5 Interview

Usability

Question: *Do you think online banking applications (Mobile banking Apps and web Banking) in Pakistan fulfill the requirement of five factors of usability i.e., learnability, efficiency, memorability, error prevention, and satisfaction?*

Table 4.1: Interview Responses for Question on Usability

Participants	Answers
1	No, it does not fulfill all the requirements because in Pakistan most banks' online services are too much poor and end-users are not happy to use online services. If users have mistakenly done a wrong transaction it's not given to whom report, users also face issues of efficiency because most of the time even after selecting the correct password users are unable to log in, and users also face difficulty after login time of inactivity.
2	No, there are some features available but only limited to memorability, etc. while no error prevention capabilities are provided and efficiency is also lacking.
3	Learnability +, Efficiency-, Memorability-, Error Prevention-, Satisfaction-.
4	Yes
5	Nope, I don't think mobile applications fulfill these five factors. The error handling is little to none in any of the banking applications, it is required to call them in case of transaction failures and 24 hours for them to respond to the request. In terms of features, a lot of banking applications lack basic features, like Bank A mobile application does not support SUI NORTHERN GAS (which is the only source of Gas in the northern region) to date. SC mobile applications even lack basic features like touch ID login.

	In terms of satisfaction, I think only 12 mobile applications are to the level where somewhat can see they're somewhat satisfactory. But in general, mobile applications are way below the threshold. They do not support basic functionality like card blocking, and logging requests (like checkbook/ATM, etc), and even good applications like that of Bank A do not support credit card blocking.
6	Yes to an extent they do. They fulfill basic needs and are easy to understand. In terms of efficiency, I would rate them somewhere like 3/5. There are issues I've had like not receiving OTP on time etc, however, many edge cases are not covered like what if I have poor signals and cannot receive OTP? I would rate this around 4/5. In terms of satisfaction, I am satisfied; however, it is not a strong satisfaction.
7	No
8	While we are very behind our international counterparts, I would say that the banking experience in Pakistan is decent. It fulfills the basic requirements and is secure.

Security

Question 1: *Do you think additional transaction passwords are needed while banking online (other than OTP)?*

Table 4.2: Responses for Question 1 on security

Participants	Answers
1	Yes, additional passwords are needed for strong security. We prefer additional passwords because it's more secure against some attacks like shoulder suffering etc.
2	Yes, a few banks provide this feature before making the transaction. They used to send half the resisted mobile number and the second half part on registered email.
3	Transaction passwords and login passwords are both a requirement based on the current threat landscape (along with OTPs).
4	Yes, they are annoying; however, they make me feel secure.
5	Yes, I think OTP is necessary but sometimes it is not enough. Having more security is always good, however, they're only useful if you're doing a transaction with someone for the first time, if they're a saved recipient, I think OTP should suffice.
6	They are needed. Let's say you're transferring an amount to a person for the first time, additional transaction passwords are necessary but in the case where we've already been sending to that specific user, it shouldn't be necessary.
7	Moreover, I think in the case of big transactions above X (like 50,000PKR) the OTP along with additional passwords should be a must.
8	Not for already added beneficiaries

Question 2: *Are you satisfied with the security features currently provided by online banking applications in Pakistan?*

Table 4.3: Responses for Question 2 on Security

Participants	**Answers**
1	Yes
2	We want some strong security features other than OTP.
3	Yes
4	Security features in banking apps are stipulated by SBP's ETGRF. If the application complies, then the security features are enough.
5	Depending on the application, some banks have an overly complicated process, like; apart from OTP, which requires the user to enter 2 passwords (1 sent via email & 1 sent via text message). This slows down the process and sometimes people might not have access to the registered e-mails.
6	Some on the other hand do not even have strong password requirements like SC.
7	Yes. I am satisfied with the terms of security features. When you login in case of a new browser, OTP is sent. When adding a new account, there is an OTP check there as well. I can reduce/increase transaction limits. Moreover, I can also add location-based transaction blocking. These things in my opinion make the application extremely helpful.
8	To an extent, they should include NFC and one-click payment solutions as well.

Usability and Security

Question 1: *Do you think the login process needs improvement while banking online in Pakistan (Mobile banking, web banking) from both a security and usability perspective?*

Table 4.4: Responses for Question 1 on Usability and Security

Participants	Answers
1	No, I think users are familiar with and compatible with the login process.
2	The login process does not need improvement in the usability domain, but in the security domain, there should be more options for security other than written passwords.
3	Yes, the login process can be improved from UI/UX side and also from a security perspective. Length, special character, password change prompting, dynamic keyboard while punching the password, and many more ways.
4	The login process is secure enough if OTPs, text passwords, and login passwords are implemented. Similarly, client-side biometrics if available can serve usability pretty well.
5	Some banking applications require you to have a separate password for mobile apps and a separate password for Web Apps. This is something that complicates things and reduces the usability aspect of the process. However, in terms of security, I think all banking applications should have a high threshold requirement for passwords, which is missing.
6	I think the current process works fine. All security measures are well placed and things shouldn't be complicated. However, I think MFA integrations (like Google Authentication) would be a good idea where OTP is not being received (in case of a lack of mobile signals).
7	The apps I am using (A and SC) both have Face ID login, which is the quickest way to log in. So I would say it's fine as it is.
8	For usability, client-side biometric availability may improve the login process.

Question 2: *Do you think authentication features like image-based passwords are more secure and convenient to use while banking online?*

Table 4.5: Responses for Question 2 on Usability and security

Participants	**Answers**
1	Yes, image-based passwords are secure as well as convenient in use because in image-based passwords there is no need for memorization.
2	From the users' perspective, it's easy and convenient. However, 1 password kind of application can be handy also.
3	No, they are a lot ambiguous, and harder to keep track of and remember. Coming up with uniqueness for different passwords/uses is highly difficult as well. Meanwhile in my opinion they do not provide any added security. Highly prone to shoulder surfing too.
4	Yes
5	I think they'll do amazing. Right now most password authentication means are based on conventional means. People are accustomed to them, which is why they're widely adopted. Image-based passwords would be a new thing; I would love to have them.
6	I think they are good when used in place of MFA/OTP. However, if this is a single mode of authentication I don't think they'll be that good when compared with conventional means.
7	No
8	It's more convenient to use

User Education

Question 1: *Do you think online banking service providers should educate users about security measures to avoid online attacks (regular updates of software, installing anti-malware software, use of strong passwords, etc.)?*

Table 4.6: Responses for Question 1 on User Education

Participants	Answers
1	Yes
2	Yes, the bank must provide information regarding security. Most users don't have enough security information on how to avoid security attacks and also updates regarding software updates as well as using anti-virus software.
3	Yes, Indeed it is very important and the bank should use some tutorials or webinars for its customers.
4	As per SBP's requirements, periodic users awareness campaigns are conducted by all banks using the alternate channel, SMS and emails, etc
5	Yes, this is extremely necessary, Majority of the people in Pakistan avoid using banking applications because they don't have adequate knowledge of it and think they'll be hacked. If adequate knowledge is provided to the customers they'll be able to understand the application while being secure and be able to fully utilize the banking experience. I believe banking application is a need of the modern era, this would help in-app adaptability as well.
6	These updates should be done forcefully in my opinion as well. Many common attacks should be explained and their prevention should be documented and educated to the customers as well.
7	Yes, frequent but not too frequent updates should be given (once a week max).
8	Yes, it's the most important issue, users should educate in this regard.

Question 2: *Do you think online banking service providers should educate users about security features to perform safe online banking (HTTPS, lock screen icon, Digital certificate, etc.)?*

Table 4.7: Responses for Question 2 on User Education

Participants	Answers
1	Yes
2	Yes, it's the most important thing for banks to educate users about online security features and also guide them on which mode of app users should use.
3	It is of utmost importance in the current time frame to avoid fraudulent transactions to secure customers as well as the bank's reputation.
4	Yes, it's already being done by all FIs/DFIs
5	I think that would be a little overkill since most of the users are laymen using the application, knowing about how HTTPS works or digital certificate works would complicate things and they'll likely avoid using the application instead.
6	I think this is necessary as well. Knowing the lock sign should be there, and the digital certificate should be there and signed are necessary to prevent any hacks, etc.
7	Yes, frequent but not too frequent updates should be given (once a week max).
8	Yes, I think users should know about all these security features to avoid phishing and other attacks.

Question 3: *Do you think online banking service providers should educate users about where to report in case of incidents/errors?*

Table 4.8: Responses for Question 3 on User Education

Participants	Answers
1	Yes
2	Yes, banks must guide users about where to report in case of incident/errors at the initial stage of any transaction (using which option in the mobile app or web-banking)
3	Yes, I guess there should be a hotline. In case of any breach, the end customer can immediately access and proceed. Banking services should communicate and educate users and this should be available in seconds.
4	There is a customer service channel; however, I believe customers should be educated in this regard too.
5	Yes, this is necessary. Right now everyone calls customer support for any issue where you have to call them and queues are high. If the mobile application itself would have the reporting issue, this would speed up things and help the users too.
6	Yes, there should be a proper plan for an incident response as well.
7	Yes, it's necessary
8	Yes, users should be educated on the top priority in this regard.

Comparison with International Online Banking Applications

Question: *Do you think that there is any difference between Pakistan and international online banking (in the security and usability domain)?*

Table 4.9: Responses for Question on Comparison between Pakistani and International Online Banking Services

Participants	Answers
1	I don't think there will be any difference in the security and usability domain.
2	Yes, there are multiple differences. In terms of online transfer from one country to another and different countries. Moreover the login process with the dynamic keyboard. Online shopping and transactions required final approval with an app notification or sending code on a registered mobile number. Online e-statement is available within mobile applications. Easy to use and a lot of features available in-app/online as compared to mobile banking in Pakistan.
3	Security features are compatible, (ETGRF is mostly based on PCI-DSS). Usability differs from platform to platform.
4	No, international chains use the same software as they have abroad.
5	I think applications in Pakistan do not have sufficient security and usability measures, I have seen a few international ones and they're very well thought out and built.
6	I haven't personally used them but from what I've heard, they have very tight security and adhere to a lot of strict and adherent locations like (in terms of credit card data ->PCI-DSS, in terms of regulations GDPR), etc.
7	No
8	Online banking apps for these banks are more or less the same abroad as well. However, there are other great banking apps such as Venmo which offer more ease of use.

Expert's Suggestion

Question: *Do you want to suggest any improvement in the security or usability domain of online banking applications in Pakistan?*

Table 4.10: Responses for Question on Suggestions for Improvement

Participants	Answers
1	Must educate users first, 2nd additional password other than OTP is necessary.
2	Activation map within your online mobile application/web application. For example, this card or account can work in ABC geographical area. Setting/editing the lower and upper limits of online and cash withdrawals month-wise and week-wise.
3	ETGRF and related regulatory and compliance requirements should be fulfilled in their true spirit. The user experience should be incorporated into the design phase too.
4	Add more features such as 1-click payment and NFC.
5	Strong Passwords (not common password, special characters, OTP), error reporting within the application, saved password- Touch/face ID authentication for faster login, intuitive menu, and the ability to manage cards must be something that is a must.
6	In terms of security, I think there should be robust pen/internal security testing. The developers should know about secure coding practices. Secure libraries should be used. Updated standards should be followed. Regulation should be followed. A sonarr cube is a tool used for code testing, this should be used. Updated and approved cryptography algorithms must be used. Latest threats and data breaches must be monitored to prevent the same issue from being caused here, this will improve the internal security by margins.
7	No need to ask for transaction passwords for already added beneficiaries.
8	Introduce one-touch pay and NFC payments. They should also look at normalizing QR payments.

4.6 Discussion of the Results

The usability results of the survey and interview are discussed in table 4.27.

Table 4.1: Usability Results of Survey and Interview

Usability	Survey	Interview
Learnability	Learnability features (guidance, manual/help features) are available and useful.	Learnability features are available and useful.
Efficiency	Users sometimes face difficulties and problems, efficiency is lacking, while using OB applications.	Expert opinions indicate that users are not fully satisfied with the efficiency of OB applications.
Memorability	Memorability features like graphics and label icons are available and helpful.	Memorability features should be available at the login phase too.
Error Prevention	Users don't know about the availability of error/incident reporting features in OB applications.	Error prevention/ error handling features should be available in OB applications.
Satisfaction	Users are not strongly satisfied.	Experts are not strongly satisfied.

The security results of the survey and interview are discussed in table 4.28.

Table 4.2: Security Results of Survey and Interview

Security	Survey	Interview
Additional Authentication	Additional authentication is needed at the time of the transaction.	Additional authentication other than OTP is needed at the time of the transaction.

The user education results of the survey and interview are discussed in table 4.29

Table 4.3: User Education Results of Survey and Interview

User Education	Survey	Interview
Security Information	Banks provide their customers with security-related information.	Very little security-related information is provided by banks for their customers. Banks should provide more education and awareness in this regard.
Security Features	The majority of users don't know about the security features provided in OB applications for security.	Users should be educated about security features provided to provide security in OB applications.
Error Reporting	The majority of users don't know about error reporting in OB applications.	Users should be educated about error reporting in OB applications.

The survey and interview results of comparison between Pakistani and international online banking applications are discussed in table 4.30.

Table 4.4: Comparison between Pakistani and International Online Banking Applications

Comparison	Survey	Interview
Comparison between Pakistani and International online banking applications in usability and security domain	Due to the limited number of responses received from international users, no clear difference was found between Pakistani and international OB applications.	Security features are more or less comparable. International online banking applications are easier to use and have more features available than OB apps in Pakistan.

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

The research work was carried out to analyse the security and usability of online banking applications in Pakistan. A review of related work showed that several factors influence the adoption of online banking applications. Some of these factors were listed frequently by different authors. The most significant among these are security and usability.

An analysis of these two factors was made using two methods. Firstly a questionnaire-based survey was carried out on Pakistani users. In this regard, 302 responses were received from Pakistanis via an online survey distribution. Secondly, an interview was carried out with eight experts to provide insight into the findings obtained in the earlier survey.

According to the findings of the survey, a total of 302 participants took part in the survey. Out of those, 224 users were using online banking applications, while 78 respondents were not using online banking applications. Results demonstrate that people are still skeptical about using online banking applications due to security, usability, and technical terminology concerns, that support [1]. The results also show that among online banking applications, mobile banking applications are the most commonly used in Pakistan.

Regarding usability, online banking applications do not fulfill all five usability features according to Nielson's model.

- **Efficiency:** As most users say that they are not familiar with all the features and functions provided in the applications, users sometimes face difficulties while banking online, especially during the login and transaction processes, which shows a lack of efficiency. An Expert's opinion also confirms that users are not satisfied with the efficient features of online banking applications.
- **Memorability:** According to interview findings, in experts' opinion, users face difficulties after a long time of inactivity as most of them forget passwords, so it takes time to get back to normal functioning while banking online.
- **Error Prevention:** According to survey results, most users do not know where to report an error or incident, and interview findings confirm that some banks do not provide these types of features, such as card blocking in mobile banking applications.
- **Satisfaction:** According to survey and interview findings, users are overall not satisfied with the usability features of online banking applications.

Regarding security analysis, the results of the survey show that the majority of users say that additional security features are necessary for online banking applications. Expert opinions confirm that additional authentication apart from OTP is needed at the time of the transaction, that support [3].

According to experts, some security features limit users e.g. requiring users to enter two passwords (one sent via email and the second sent via text message). This type of security feature slows down and complicates online banking for users. The results also show that

users are satisfied with the login process because users are more comfortable with commonly used authentication features. However, experts suggest the inclusion of secure and usable biometric authentication (like fingerprints and face recognition). This suggestion is also supported by Oliver Buckley and Jason R.C. Nurse, 2019, [7]. The findings from the survey demonstrate that image-based passwords are convenient to use, but according to experts' opinions, image-based passwords should be used as a second authentication option only. They should never be used as a single source of authentication.

This research also finds that both usability and security are equally significant in online banking applications in Pakistan. At present users are not familiar with most of the security features and information provided to protect and conduct secure online banking. Expert opinions also confirm the survey findings that users should be educated about security features and security measures to avoid becoming targets of online attacks. The survey results show that most users do not know where to report in case of an error or incident. An expert's opinion also confirms the finding that online banking service providers should communicate and educate users about proper reporting procedures (by using which option in mobile app and web banking) in case of error or incident. These options should be available in seconds.

As only a small number of international online banking users took part in the survey it is infeasible to generalize the differences between Pakistani and international online banking applications, particularly in terms of security and usability. However, the data does indicate that international online banking applications provide more functionality as compared to Pakistani online banking applications. According to experts' opinions, security features in

Pakistan are comparable with international online banking applications, while usability features varied from country to country.

5.2 Recommendations

The results suggest that improving security, usability, and user education can increase the adoption of online banking applications in Pakistan.

The results also show that users require stronger and more usable authentication features, especially in the transaction phase. In the usability domain, online banking service providers should prioritize the five usability factors.

It was also found that the error prevention factor is missing in most online banking applications. In the cases where it is available users are unaware of its presence. Online service providers should provide these error reporting facilities for users within the applications, also these features should be available within a fraction of a second.

Efficiency and memorability factors also need improvement. In some cases, users face difficulties while receiving OTP due to lack of signals, unavailability of registered source for receiving OTP/emails, and the need for additional devices, so there should be some built-in option for additional authentication like an additional password. This additional password should not be image-based but it should be usable and efficient.

Most users were satisfied with how memorability was provided. Almost all the service providers provide label icons and graphics; however, users mostly face difficulties in using applications after a long time of inactivity because they have forgotten their passwords. All service providers should provide touch-ID and face-recognition as login options in online

banking applications. By implementing these recommendations, higher user satisfaction can be achieved in online banking applications in Pakistan.

Lastly, the user should be educated about security measures, security features, and error reporting. According to SBP users' awareness campaigns, adequate knowledge should be provided to the customers so they can understand the application and fully utilize it securely. As recommended by one expert, the design phase of the banking application should incorporate user experience, and related regulatory and compliance requirements (e.g. Enterprise Technology Governance and Risk Management Framework ETGRF) should be fulfilled in its true spirit.

5.3 Future Work

Future work can include the security and usability analysis of online banking services like one-touch pay, NFC, and QR payment systems. Researchers can also investigate which aspects of security and usability contribute to unfavorable attitudes toward accessing these services, as well as how attitudes might be changed to make these services more likely to be used. Furthermore, a more thorough exploration can be made to understand the user experiences and perceptions of these online banking services in Pakistan.

REFERENCES

[1] FN Mahmadi, Z. Z. (2016). “Computer Security Issues in Online Banking: An Assessment from the Context of Usable Security”. IOP Conf. Series: Material Science and Engineering (p. 12). IOP.

[2] Mayhew, M. M. (2014). "Security and Usability of Authenticating Process of Online Banking: User Experience Study'. International Carnahan Conference on Security Technology (ICCST) (p.6). IEEE.

[3] Aleksandra Svilar, J. Z. (2016). "User Experience with Security Elements in Internet and Mobile Banking". Sustainable Organization (p. 10). DE GRUYTER.

[4] M.K.Normalini, T. S. (2019). "Investigating the Impact of Security Factors In E-business and Internet Banking Usage Intention among Malaysians". Industrial Engineering & Management Systems, 10.

[5] Yan Xiao, A. S. (2017). "Factor Influencing People's Intention to Adopt E-Banking: An Empirical Study of Consumers in Shandong Province, China". Asian Journal of Computer and Information Systems, 19.

[6] Anoud Bani-Hani, M. M. (2019). "Online Authentication Methods Used in Banks and Attacks Against These Methods". Procedia Computer Science (p. 8). ELSEVIER.

[7] Oliver Buckley, J. R. (2019). "The language of biometrics: Analysing public perceptions". Journal of Information Security and Applications, 8.

[8] Armend Salihu, H. M. (2019). "The Effects of Security and Ease of Use on reducing the problems/deficiencies of Electronic Banking Services". IFAC (p. 5). ELSEVIER.

[9] Nikola Milosavljevic, S. N. (2019). "Customer perception of information security in internet banking". SENET (p. 6). ATLANTIS PRESS.

[10] Anum Tanveer Kiyani, A. L.-R. (2020). "Secure Online Banking With Biometric”. International Conference on Advances in the Emerging Computing Technologies (AECT) (p. 6). IEEE.

[11] Ms.Aria, M. A. (2020). "Secure Online Payment with Facial Recognition using MTCNN. International Journal of Applied Engineering Research, 4.

[12] Abiodun Esther Omolara, A. J. (2019). "FingerEye: improvising security and optimizing ATM transaction time based on iris-scan authentication". International Journal of Electrical and Computer Engineering (IJECE), 8.

[13] Singh, V. K. (2019). "Implementation of an Additional Factor for Secure Authentication in Online Transactions". Journal of Organizational Computing and Electronic Commerce.

[14] Lokesh Sharma, M. m. (2018). "Mobile Banking Transaction using Fingerprint Authentication". ICISC (p. 6). IEEE.

[15] Tahir Mehmood. (2020). "Usability and Security in Internet Banking Password (Survey)". International Journal of Science & Engineering Research, 6.

[16] Kamaludin, N. S. (2015). "Using Pre-Test to Validate the Questionnaire for Website Usability (QWU). ICSECS (p. 5). IEEE.

[17] Joyce Soares, A. (2016). "Fingerprint and Iris Biometric Controlled Smart Banking Machine Embedded with GSM Technology for OTP". ICACDOT (p. 6). IEEE.

[18] Ijar, V. M. (2016). "Secure PIN Authentication for ATM Transaction using Mobile Application". International Journal of Soft Computing and Engineering.

[19] Samir Chabbi, R. B. (2020). "Dynamic array PIN: A novel approach to secure NFC electronic Payment between ATM and Smartphone". Information Security Journal.

[20] Odoh, E.N. (2015). "Security Issues Analysis on Online Banking". *International Journal of Computer Science and Telecommunications*, 8.

[21] Mathias Mujinga (2020). "Online Banking Service Quality: A South African E-S-QUAL Analysis". (IFIP) International Federation for Information Processing (p.228-238).Springer.

[22] Introduction to usability. https://www.nngroup.com/articles/usability-101-introduction-to-usability/.

[23] M. F. Mridha, K. N. (2017). "A New Approach to Enhance Internet Banking Security". *International Journal of Computer Applications*, 6.

[24] O. R. Vincent, T. M.-A. (2020). "An Identity-Based Elliptic Curve Cryptography for Mobile Payment". *SN Computer Science* (p. 12). Springer.

[25] Security Mechanisms. https://www.rbc.com/privacysecurity/ca/security-mechanisms.html

[26] Rastari, A. B. (2015). "A Model for Increasing Usability of Mobile Banking Apps on SmartPhones". *Indian Journal of Science and Technology*, 9.

[27] Privacy. https://en.wikipedia.org/wiki/Privacy

[28] Yunus Barlas, O. E. (2020). "DAKOTA: Continuous Authentication with Behavioral Biometrics in a Mobile Banking Application". *5th International Conference on Computer Science and Engineering (UBMK)* (p. 6). IEEE.

[29] Authentication. https://techterms.com/definition/authentication

[30] Arthi. J, A. (2016). "GeoMoB – A Geo Location based browser for secured Mobile Banking". *International Conference on Advanced Computing (ICoAC)* (p. 6). IEEE.

[31] Jakob Nielsen. (1996). "Usability Metrics: Tracking Interface Improvements", (p. 2). IEEE.

[32] Wadie Nasri, Laouar Charfeddine. (2012). "Factors affecting the adoption of Internet banking in Tunisia: An integration theory of acceptance model and theory of planned behavior". Journal of High Technology Management Research (p.14). ELSEVIER.

[33] Online banking. https://www.investopedia.com/terms/o/onlinebanking.asp

[34] Pakistanis shifted to the internet, and mobile banking. https://tribune.com.pk/story/2239324/2-pakistanis-shift-internet-mobile-banking

[35] Qualitative vs Quantitative data. https://www.g2.com/articles/qualitative-vs-quantitative-data

[36] Analysis tools. https://nagt.org/nagt/geoedresearch/toolbox/analysis_tools/index.html

[37] Structured vs unstructured interviews: https://sociology-tips.com/library/lecture/read/131673-what-is-structured-and-unstructured-questionnaire

[38] Fisher, C., 2007. Researching and writing a dissertation: a guidebook for business students. 2nd ed. Harlow: Prentice-Hall.

[39] Quote https://www.brainyquote.com/quotes/suze_orman_465794

[40] Valentyna Yakubiv, R. S. (2019). "Development Of Electronic Banking: A CASE STUDY OF UKRAINE". *ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES*, 219-232.

[41] Nur Azimah bt Mohd, Zarul Fitri Zaaba, (2019). " A Review of Usability and Security Evaluation Model of E-commerce Website" The Fifth Information System International Conference, (1199-1205). ELSEVIER.

APPENDIX A

Appendix A contains the questionnaire that was used to collect responses from users and non-users of online banking applications in Pakistan.

1. Screening Survey

2. What is your gender? *
- Male
- Female

2. What is your age? *
- 18-24 years old
- 25-34 years old
- 35-44 years old
- 45-55 years old

3. What is the highest education level you have completed? *
- High School
- College
- Bachelor
- Masters
- PHD

4. How would you rate your general computer expertise? *
- Very good
- Good
- Fair
- Poor
- Very poor

5. How would you rate your computer security expertise? *
- Very good
- Good
- Fair
- Poor
- Very poor

6. What is your nationality? *
- _____

7. Do you use online banking? *
- Yes
- No

Logic: Section "2" is hidden if "Do you use online banking?" is "Yes"

2. Non-users

Description: Reasons for not using online banking

1. What are your main reasons for not using online banking? *

- Concerned about security (don’t trust online banking)
- Don’t get on with technology
- Not available through my bank
- Never hear of online banking
- It's difficult to use (usability issues)
- Other _____

3. Users of Online Banking

1. In Pakistan, which bank do you use for most of your online banking services? *

- Meezan Bank
- Habib Bank
- United Bank Limited
- Bank Alfalah
- Askari Bank
- None (i am not using any Pakistani bank for online banking)
- Other _____

Logic: Section "6" is open if "In Pakistan, which bank do you use for most of your online banking services?" is "None"

2. Who recommended you to use online banking? Select all that apply. *
- Family member
- Working organization
- Friends
- Bank
- Other_____

3. How frequently do you physically visit your bank branch per month? *
- Less than 1
- 1 to 3 times
- 4 to 8 times
- Over 8 times

4. How often do you use online banking? *
- Daily
- 2 to 3 times per week
- Monthly
- Rarely

5. Which online banking application do you commonly use? Select all that apply. *
- Mobile Banking App
- Web Banking
- Credit card
- Other _____

6. Do you think that using online banking is entirely within your control? *
- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

4. Usability analysis of online banking applications

1. Do you face any difficulties and/or problems when using online banking applications (e.g. unable to login, transfer money, etc.)? *
- _____

2. Do you know how to find informative guidelines, manuals, or how to use help features while using online banking applications? *
- Yes
- No

Logic: The following question no 3is hidden if "Do you know how to find informative guidelines, manuals, or how to use help features while using online banking applications?" is "No"

3. Do you find manual/guidance/help features useful? *
- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

4. Do you know all the features/functions provided in online banking applications? *
- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly agree

5. Does your online banking application use graphics and helpful label icons for the convenience of customers using the application after a long time? *
- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

6. If you wanted to report a security breach or ask a question about the security of an online banking application, where would you do this (e.g. block/unblock debit card)? *
- _____

7. Do you think online banking applications in Pakistan are complicated for non-technical users? *
- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

8. Do you think that the authentication features limit you when you use banking online applications? *

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

5. Security analysis of online banking

1. Do you know the correct web address of your bank? *
- Yes
- No
- Not sure
- Other____

2. In Pakistan, which authentication mechanism(s) does your bank mostly use for online banking applications? Select all that apply. *
- Username, Password
- PIN
- Image-based Password
- Fingerprints
- Face recognition
- Other___

3. Do you use the same password for different online banking applications? *
- Yes
- No
- Sometimes

4. Does your bank provide its customers with security-related information/guidelines? (e.g. regular update of software, use of strong passwords) *
- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

5. Does your bank verify your password for each online banking application separately (instead of allowing you to use the same password for all its online banking applications)? *
- Yes
- No
- I don’t know

6. Do you know the various security features used by your online banking applications (e.g. digital certificate, HTTPS, lock icon, etc.)?
- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

7. Does your online banking application require additional authentication at the time of the transaction (e.g. image-based password, security question, one-time password, transaction password, etc.)?*
- Yes
- No
- I don't know

8. Do you think that additional authentication is needed (e.g. during transactions)? *
- Yes
- No
- I don't know

9. Do you think convenience or security is more important for you when using banking online applications? *
- Convenience
- Security
- Both are equally important
- Neither

10. How concerned are you about the security of online banking? Keep in mind that "security" means privacy, confidentiality, and proof of identity. *
- Not at all concerned
- A little concerned
- Concerned
- Very Concerned

11. Which security measures are best for securing you against various kinds of online banking attacks? Select all that apply. *
- Self-awareness in security
- Installing anti-malicious software
- Limiting online activities
- Users education
- Keeping software up to date
- Other _____

12. Which authentication features do you think are not necessary for securing your online banking applications? Select all that apply. *
- Password length
- Uncommon password
- Complex password
- Password Change frequency
- Secret image
- Security question
- None
- Other_____

13. Do you feel secure sending sensitive information during online banking applications? *
- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

14. Are you satisfied with the security features currently provided by the online banking applications you use? *
- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

15. Are advanced authentication methods used in your online banking applications? (Note: Simple authentication methods include passwords while advanced authentication methods include iris scan and facial recognition.) *
- Yes
- No
- I don’t know

6. Foreign Online Banking

1. Are you using any foreign bank account for online banking?

- Yes
- No

Logic: The remaining sections are hidden, if “Are you using any foreign bank account for online banking?” is “No”. (Submit survey)

7. Foreign Online Banking

1. Which foreign online bank do you use (e.g. National Bank of Dubai, United Arab Emirates)?*

- _____

2. Does your foreign bank allow you to create an account without physically visiting the bank (online account creation)? *

- Yes
- No
- I don't know

3. Do you find any difficulties and problems while dealing with your foreign online banking (e.g. unable to login, transfer money, etc.)? *

- _____

4. Do you know how to find informative guidelines, manuals, or how to use help features while using foreign online banking applications? *

- Yes
- No

Logic: question 5 is hidden if "Do you know how to find informative guidelines, manuals, or how to use help features while using foreign online banking applications?" is "No"

Foreign Manual Helpful

5. Do you find manual/ guidance/help features useful? *

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

8. Usability Analysis of Foreign online banking

1. Do you know all the features/functions provided in your foreign online banking applications? *

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

2. Do your foreign online banking applications use graphics and helpful label icons for the convenience of customers using the applications after a long time? *

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly agree

3. In foreign online banking, if you wanted to report a security breach or ask a question about the security of an online banking application, where would you do this (e.g. block/unblock debit card)? *

- _____

4. Do you think online banking applications in foreign are complicated for non-technical users? *

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

5. Do you think that the authentication features limit you when you use foreign banking online applications? *

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

9. Security analysis of foreign online banking

1. Do you know the correct web address of your foreign bank? *
- Yes
- No
- Not Sure
- other _____

2. Which authentication mechanism(s) does your foreign bank mostly use for online banking applications? Select all that apply. *
- Username, Password
- PIN
- Image-based Password
- Fingerprint
- Face recognition
- other _____

3. Do you use the same password for different foreign online banking applications?*
- Yes
- Sometimes
- No

4. Does your foreign bank provide its customers with security-related information/guidelines (e.g. regular update of software, use of strong passwords)?
- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

5. Do you think that your foreign online banking applications are convenient to use as compared to Pakistan's online banking applications?*
- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

6. Does your foreign bank verify your password for each online banking application separately (instead of allowing you to use the same password for all its online banking applications)?*
- Yes
- No
- I don’t know

7. Do you know the various security features used by your foreign online banking applications (e.g. Digital Certificate, HTTPS, lock icon, etc.)? *
- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

8. Does your foreign online banking application require additional authentication at the time of the transaction (e.g. image-based password, security question, one-time password, transaction password, etc.)? *
- Yes
- No
- I don't know

9. Do you think that additional authentication is needed (e.g. during transactions) in foreign online banking applications? *
- Yes
- No
- I don't know

10. Which authentication features do you think are not necessary for securing your foreign online banking applications? Select all that apply. *
- Password length
- Uncommon Password
- Complex Password
- Password Change Frequency
- Secret Image
- Security Question
- None
- Other _____

11. Do you feel secure while sending sensitive information during foreign online Banking? *
- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

12. Are you satisfied with the security features currently provided by the foreign online banking applications you use? *
- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

13. Are advanced authentication methods used in your foreign online banking applications (Note: Simple authentication methods include passwords while advanced authentication methods include iris scan and facial recognition.)? *

- Yes
- No
- I don’t know