

Relationship between Mobile Banking Applications Security and User Trust

B.G.D Tharangani

189473V

Faculty of Information Technology

University of Moratuwa

August 2021

Relationship between Mobile Banking Applications Security and User Trust

B.G.D. Tharangani

189473V

Dissertation submitted to the Faculty of Information Technology, University of Moratuwa, Sri Lanka for the partial fulfillment of Degree of Master of Science in Information Technology.

August 2021

Declaration

It is hereby declared by us that this thesis is our own work. Further this research has not been submitted in any other form for another degree or diploma at any university or other institution of tertiary education. Acknowledgements have been given for the information derived from the published or unpublished work of others in the text and a references list is also given.

Name of Student:

B.G.D. Tharangani

Signature of Student:

Date:

Name of Supervisor:

Ms. Indika Karunarathna

Signature of Supervisor:

Date:

Acknowledgement

First and foremost, my sincere gratitude goes to my research supervisor Ms. Indika Karynarathne. She gave me invaluable guidance and instructions for me to successfully complete this research. Without her guidance this research would never be a success.

I would also like to pay my gratitude to all the members my research evaluation panel for their important instructions and recommendation given to me from the interim stage.

Finally, I would like to thank my family members for the support given to me.

Abstract

Banking industry has become one of the most vibrant industries at present with the expansion of economies and complication of human needs and wants. One of very interesting technological innovations for these online transactions is performing them through smart phone mobile applications. Though these mobile banking applications are very popular in today's context and they derive various advantages, concerns have also arise regarding the security of the banking transactions done through mobile banking applications. Therefore, mobile banking applications security has become one of the issues of paramount importance for mobile applications developers and service providing banks. According to literature related to this area of concern, many researchers recognise security as a strong reason for the banking customers for not adopting to mobile banking applications. Those reearchers highlight that one of the main reasons for lower adoption for mobile banking and lower usage of mobile banking applications is the concers of security.

There is a gap in emperical knowledge with respect to the relationship between the degree of security of mobile banking applications and user trust. When it comes to the Sri Lankan context, the gap in emperical knowledge about the above factor is very obvious. Apart from that, the preliminary observations done by the researcher revealed that many people are reluctant to use mobile banking applications. Although many banking customers own smart devices and have a fair knowledge in operating smart devices, they are still reluctant to install mobile banking applications and exploit the opportunity to perform the banking transactions easily through the app. It made this researcher to study about the issue and refer related literature. According to literature, the reason for this lower adoption for mobile banking applications is a trust issue that mobile banking customers have regarding the security of mobile banking applications. Therefore, the researcher thought of investigating whether there is a relationship between degree of security of mobile banking applications perceived by the users and user trust.

One hypothesis formulated with the idea of coming up with findings for the research problem spoken in this research. The research was conducted connecting with 220 individuals representing executive category of both public and private sectors. The

conducted research was a correlation study and it is a cross sectional study as well. The unit of analysis was individual level. Frequency analysis was used to understand the sample profile and descriptive statistics were used to investigate the extent of perception regarding the security of mobile banking applications and user trust. Correlation analysis was used to test the hypothesis.

The results showed that there is a strong positive correlation between perceived degree of security of mobile banking applications and user trust. This research revealed that the most sought trust element by the customers is benevolence. It was also revealed that access control systems and ability to perform transactions through the application are the most important existing security control measures for the customers. The research further revealed that customers expect banks to add multi factor authentication and fingerprinting technology to mobile banking applications when developing security of mobile banking applications in the future.

This research is beneficial for the banks and mobile banking applications developers to get a better understanding about the relationship between security of mobile banking Applications and user trust. Through the findings of this research bankers get a better understanding on what security features they should enhance and what security features they should include in future developments of mobile banking applications. Thus this research provides simple guidelines for the banks and developers to develop efficient and effective mobile banking applications that ensure surety of the transactions of the users and gain user trust.

Table of Contents

Declaration.....	i
Acknowledgement	ii
Abstract.....	iii
Table of Contents.....	v
List of Tables	viii
Table of figure.....	ix
CHAPTER 1	1
1 Introduction	1
1.1 Research Background.....	2
1.2 Problem Statement	6
1.3 Research Questions	9
1.4 Research Objectives	9
1.5 Hypothesis.....	10
1.6 Sampling Design	10
1.7 Data Analysis	10
1.8 Significance of The Study	10
CHAPTER 2	13
2 Literature Review	13
2.1 A Critical Overview	13
2.2 History And Origins of The Concept of Mobile Banking.....	14
2.3 A Definitional Approach For Mobile Banking	15
2.4 Mobile Banking Services	16
2.4.1 Information about accounts:	17
2.4.2 Fund Transfers and Bill Payments:.....	17
2.4.3 Services on Investment:	17
2.4.4 Support Services:	18
2.4.5 Contented Services:	18
2.5 Platforms of Mobile Banking.....	18
2.5.1 WAP Banking	18
2.5.2 SMS Banking	18
2.5.3 Standalone Applications	19
2.6 Mobile Banking Applications	19

2.6.1	Advantages Of Mobile Banking	21
2.6.2	Disadvantages Associated with Mobile Banking	22
2.7	Security Of Mobile Banking	23
2.7.1	Types Of Security Related Threats for Mobile Banking	24
2.7.1.1	Rootkits	26
2.7.1.2	Social Engineering Attacks	26
2.7.1.3	Resource Abuse Attacks.....	27
2.7.1.4	Data Loss.....	27
2.7.1.5	Data Integrity Threats.....	27
2.8	User Trust.....	27
CHAPTER 3		30
3	Conceptualization, Operationalization and Methodology	30
3.1	Conceptualization.....	30
3.1.1	Theoretical Framework.....	30
3.1.1.1	Working Definitions of the Variables	32
3.1.1.1.1	Security Of Mobile Banking Applications	32
3.1.1.1.2	Trust of The Mobile Banking Users	33
3.1.2	Hypothesis.....	33
3.1.2.1	Hypothesis 1	33
3.2	Operationalization	35
3.2.1	Operationalization Of Mobile Banking Applications Security.....	35
3.2.2	Operationalization Of User Trust.....	35
3.2.3	Operationalization Of Frequency Of Mobile Banking Applications Usage	36
3.2.4	Gender.....	37
3.3	Methodology	37
3.3.1	Purpose Of The Study	37
3.3.2	Type Of Investigation	37
3.3.3	Study Setting And Unit Of Analysis.....	37
3.3.4	Methodological Choice	37
3.3.5	Population	38
3.3.6	Sample.....	38
3.3.7	Data Collection Methods	38
3.3.8	Data Presentation And Analysis	38

CHAPTER 4	39
4 Data Presentation and Data Analysis.....	39
4.1 Introduction	39
4.2 Univariate Analysis	39
4.2.1 Frequency distribution analysis of respondents by their personal characteristics	39
4.2.1.1 Composition of the sample according to gender	40
4.2.1.2 Composition of the sample according age groups	41
4.2.2 Descriptive statistics	42
4.2.2.1 Mean and standard deviation of perceived degree of security of mobile banking applications	43
4.2.2.2 Mean and Standard deviation of user trust.....	43
4.3 Bivariate Analysis	44
4.3.1 Correlation analysis	44
CHAPTER 5	50
5 Discussion, Conclusions and Recommendations	50
5.1 Introduction	50
5.2 Discussion On Findings	50
5.2.1 Finding One	50
5.2.2 Finding Two.....	51
5.2.3 Finding Three.....	51
5.2.4 Finding Four.....	52
5.2.5 Finding Five	53
5.2.6 Finding Six.....	53
5.3 Conclusion and Recommendations	54
5.4 Limitations of the research.....	57
5.5 Further research area	57
References.....	58

List of Tables

Table 3-1: Operationalization of Security of Mobile Banking Applications.....	35
Table 4-1: Gender Distribution.....	40
Table 4-2: Distribution According to the Age Groups	41
Table 4-3: Mean And Standard Deviation Coefficients of Perceived Degree of Security of Mobile Banking Applications	43
Table 4-4: Mean And Standard Deviation Coefficients of User Trust	43
Table 4-5: Correlation Between Perceived Degree of Security of Mobile Banking Applications and User Trust	44
Table 4-6: Ranking of Credibility	45
Table 4-7: Ranking of Benevolence	46
Table 4-10: Most Important Security Feature.....	48
Table 4-11: Most Anticipated Security Feature.....	49

Table of Figure

Figure 2.1: A Typical Threat Scenario for Mobile Banking Apps	25
Figure 3.1: Theoretical Framework	31
Figure 4.1: Gender Distribution	40
Figure 4.2: Distribution According to the Age Limits of the Users	41
Figure 4.3: Ranking of Credibility	45
Figure 4.5: Ranking of Structural Assurances	46
Figure 4.6: Ranking of Firm Reputation.....	47

CHAPTER 1

1 Introduction

Banking industry has become one of the most vibrant industries at present with the expansion of economies and complication of human needs and wants. Unlike in the past, in today's context banks have widely used technology to enhance the efficiency and effectiveness of its operations. All the institutions which are operated in the banking sector have introduced many innovative solutions, mainly based on modern technology, to their customers with the idea of fulfilling the requirements of them in an efficient and effective manner.

Recent developments in the telecommunication sector have made significant influences to the banking sector. Bloom in the smart phone market is one such much affected influences. In today's context smart devices such as smart phones and tabs have become one of the most popular tangible items in the world. Literally there is a smart device in every person's hand today. Improved hardware and modern improved software have enhanced the growth of the smart device industry. As a result, influence of smart device usage has made much influence to banking industry as well.

At present, market conditions are very competitive and highly turbulent. In such environment, all the business organizations are trying to achieve competitive edge for their products and services. Being a service, banking and finance is also the same in this context. Unlike in the past, people are very busy in their lives as a result of complicated needs and wants. Therefore, lots of people prefer online transactions to purchase the goods and services that are needed to satisfy their needs and wants. This is mainly because of the facts that online transactions are much convenient and time saving.

One of very interesting innovations for these online transactions is performing them through smart phone mobile applications. Mobile applications can be understood as a software application or else a computer program which has been designed to run through a mobile platform or device such as smart phones, tabs etc. banks have utilized this mobile

app technology to a good effect by introducing banking facilities through mobile applications. At present, almost all the banks operated in the market have developed mobile applications which enable their customers to download the application in to their mobile devices and perform bank transactions such as balance checking, fund transfers, bill payments etc.

Though these mobile banking applications are very popular in today's context and they derive various advantages, concerns have also arised regarding the security of the banking transactions done through mobile banking applications. Therefore, mobile banking applications security has become one of the issues of paramount importance for mobile applications developers and service providing banks. Banks are very keen on maintaining proper level of security in the mobile banking applications that they introduce to their customers. Apart from that, several researches have been done about the impact of the level of mobile banking applications security which financial institutions like banks introduce to their customers to the trust of the mobile banking customers. However, in Sri Lankan context there is a lack of research in this regard. Therefore, in this research the researcher attempts to fulfill that gap by investigating how security of mobile banking applications impact on trust of the customers who use mobile banking. Here, the researcher is in a view that knowledge disseminated through this research would be very beneficial for the banks and mobile applications developers to understand the relationship between mobile banking applications security and user trust enabling banks to make decisions about the security enhancements of their mobile banking applications and by that enhance customer satisfaction. This chapter is dedicated to explain about the background and problem identification, objectives of the research, methodology of carrying out the research and significance of this research for the respective field.

1.1 Research Background

Unlike in the past, at present banking industry has achieved tremendous advancements in technology and it has made the customers very convenient to perform their banking related transactions. Some of these technological enhancements include green banking accounts, real time settlement, inter banking facilities, internet banking and mobile banking. Lots of banks come up with many innovative solutions based on the computer and

telecommunication technologies to deliver an excellent service to their customers and thus gain a competitive advantage in the market.

It is quite evident that in today's society there is a smart device in every hand regardless of gender, age or economic status. Most people are very familiar with various mobile applications available in their smart devices. Banks have taken steps to utilize this opportunity into good effect through the introduction of online banking facilities through mobile apps. In alternate terms, this is called mobile banking. In Sri Lanka as well we can see almost all the commercial, savings and development banks have provided their customers with this facility. In today's context, people spend busy life styles as a result of the complicated needs and wants they have. Therefore, people tend to move for smart ways of doing things to manage time. Lots of people prefer online transactions to purchase the goods and services that are needed to satisfy their needs and wants and this is why mobile banking applications become very popular.

Mobile applications can be referred to as a software application or else a computer program intended to work on a mobile device. At present, almost all the banks operated in the market have developed mobile applications which enable their customers to download the application in to their mobile devices and perform bank transactions such as balance checking, fund transfers, bill payments etc.

Muccini et al (2010) express that applications running on mobile devices are are very popular these days in such a way that dipict a revolution in the information technology field. Apart from that Harrison et al (2013) further explains "Advances in mobile technology have enabled a wide range of applications to be developed that can be used by people on the move". Presenting a definition for mobile applications Muccini et al (2010) defines mobile banking applications as "an application running on mobile devices and taking in input contextual information". Adding further, the authors highlight that mobile applications were initially developed mostly in the sector of entertainment, those are currently being introduced at various critical fields. Mobile banking concept can be introduced as one such domain.

“Mobile Banking can be defined as a channel whereby the customer interacts with a bank via a mobile device” (Barnes & Corbit, 2003). Referring to Laukkanen and Passanen (2008), Akturan & Tezcan (2011) describe mobile banking as a channel through which a consumer interacts with a bank or financial institution through a mobile device, such as a mobile phone or tab. Adding some more clarification to the definitions of mobile banking Pandey (2019) explains that mobile banking can be referred to the use of a smartphone or other mobile device to perform online transactions. This service is supplied by the bank. Unlike internet banking, mobile banking uses software programs called applications. Apart from that mobile banking is open for the entire 24x7. Somehow, mobile banking is dependent on the availability of an internet or data connection to the mobile device.

The same above author bring out some important facts regarding the history of mobile banking. According to him the initial form of mobile banking is transactions done through short message service that was well recognized as SMS Banking. After that smartphone were introduced to the market embedded with Wireless Application Protocol (WAP) support enabling the use of the mobile web. Then European banks primarily started submission mobile banking using WAP technology for the customers. As highlighted by the author, it was in 2011 that fully functioning banking app was firstly launched by RBS. Firstly, it was available only in apple devices but later it was expanded to blackberry and android devices as well. The journey started like that has now reached to a very largely used and highly popular way of banking.

Being started its journey as explained above, mobile banking applications are now widely used in almost all the countries in the world and it has become one of the most convenient ways of banking as far as today’s highly vibrant environment situations are concerned. Applications designed for mobile banking can be generally identified as a mobile software application that enables banking transactions to be performed. Bringing up a quite comprehensive definition for mobile banking, Alafeef, Singh, & Ahmad (2011) describe that “mobile banking applications are type of execution of financial services in the course of which within an electronic procedure the clients use mobile communication techniques in conjunction with mobile devices”. These mobile banking applications provide electronic

platform for its users to perform banking businesses such as bill payments, transfer of funds and balance checking. Although the use of mobile banking applications have become widely popular as a result of the convenience provided by those for today's turbulent environment, many concerns also have been arisen regarding various aspects of mobile banking and use of mobile banking applications. One such issue of paramount importance can be identified as the concerns arisen based on the level of security of the transactions done through such applications. According to Rouse, M (2013), degree of security of mobile banking applications is the level of defense that mobile applications have from malware and the activities of hackers and other criminals. Security of mobile banking can also refer to different types of technologies and production practices which minimize the risk of exploiting mobile devices through their apps. Adding some further clarifications to the subjected phenomenon, the author states that a mobile device has several components and all of them are vulnerable to weaknesses of security. These various parts are made, distributed and used by various players. Each of this part plays an important role the security of a device. Each of such player should integrate security procedures into mobile devices as they are designed and built, and into mobile apps as they are considered and written, but these tasks are not always sufficiently carried out. Architectural flaws, device loss or theft, platform weakness, isolation and permission problems and application weakness can be understood as common vulnerabilities for mobile devices.

Unfolding some further aspects about mobile banking security FraudWatch International (2019) suggests that security of mobile applications is denoted by the ways and means of safeguarding mobile device applications from digital fraud such as malware, hacking and other types of criminal manipulation. Security related to mobile applications shall be executed by both technological means together with personal responses and business procedures envisioned to defense digital integrity on mobile devices. Level of security of the mobile banking applications have become one of the salient aspects in winning the trust of the users of such applications.

Findings of the research carried out by Kaya (2013) recognise one factor as a strong reason for the users of mobile banking applications not to adopt mobile banking and it is their concerns for security. The same author highlights that one of the main reasons for lower

adoption for the use of mobile banking applications is the concerns of security. Apart from that in their research findings Kim et al (2009) point out that relative paybacks, tendency to trust and security guarantees had a significant effect on initial trust of mobile banking. Therefore, it is quite clear that security of mobile banking applications play a vital role in gaining customer trust.

These are some of the areas of great importance as far as ICT research areas are concerned. Knowledge generated through such research can contribute in a great deal for the enhancement of mobile phone applications security and it would provide a strategic mechanism for the banks to address this key issue. Though there are some research-based literatures are available in global context with respect to mobile phone applications security and how it may be affected to customer trust, there is a serious deficit in empirical evidence in Sri Lankan context for this area. Therefore, through this study, the researcher attempts to contribute in a productive way to fill this gap of empirical evidence in mobile banking application security and how mobile bank application user trust is affected by the perception about the security of apps used for mobile banking which they use.

1.2 Problem Statement

“Mobile Banking can be defined as a channel whereby the customer interacts with a bank via a mobile device” (Barnes & Corbit, 2003). Mobile banking is one of the most important innovative solutions in today’s dynamic environment factors are concerned since it provides very convenient ways and means for performing banking transactions. With the rapid growth of the mobile device technology such as mobile phones, tablets and other smart mobile platforms now mobile banking has achieved a revolutionary development from performing transactions through SMS and WAP to mobile applications. Mobile banking applications are now widely used in almost all the countries in the world and it has become one of the most convenient ways of banking. Mobile banking applications could be identified generally as a mobile software application which enables banking transactions to be performed. These mobile banking applications provide electronic platform for its users to perform banking dealings such as bill payments, fund transfers and account balance checking.

Although the use of mobile banking applications have become widely popular as a result of the convenience provided by those for today's turbulent environment, many concerns also have been arisen regarding various aspects of mobile banking and use of mobile banking applications. One such issue of paramount importance can be identified as the concerns arisen based on the level of security of the transactions done through such applications. According to Rouse, M (2013) "mobile app security is the extent of protection that mobile device applications (apps) have from malware and the activities of crackers and other criminals"

In Sri Lankan context as well, literally every commercial bank has developed and introduced mobile banking applications for their customers. Those mobile banking applications offer a wide range of services where customers can just stay at home or office and perform their banking transactions through the app. Even though the situation is like this, this researcher observed that many people are reluctant to use mobile banking applications. Although many banking customers own smart devices and have a fair knowledge in operating smart devices, they are still reluctant to install mobile banking applications and exploit the opportunity to perform the banking transactions easily through the app. Still most of the banking customers prefer to go to the bank physically, stay in counters, fill in various forms and banking slips and do their banking transactions manually. The researcher also observed that, even those customers who have installed mobile banking applications tend to use it less. Even in a pandemic situation like Covid 19 where people are strictly advised to limit travelling and ensure social distancing, it is observed that people are still waiting in queues at banks to do their banking transactions risking their lives as well. They can simply use mobile banking applications and perform their banking transactions being at homes in a pandemic situation like this. Therefore, the researcher thought it is interesting to investigate why people are still going physically to banks risking their lives as well in a pandemic situation while they are having simple methods like using mobile banking applications to do their transactions. These observations made this researcher to refer literature about mobile banking applications to find out a possible reason for this. When referring to literature, this researcher came across the following important factors.

Kaya (2013) recognises that one factor as a strong reason for the users of mobile banking applications not to accept mobile banking and it is their concerns for security. The same author highlights that one of the main reasons for lower adoption for mobile banking and use of mobile banking applications is the concerns of security. Apart from that in their research findings Kim et al (2009) point out that relative paybacks, tendency to trust and security guarantees had a significant outcome on primary trust of mobile banking. On the other hand, findings of the study carried out by Jabri & Sohail (2012) shows that “perceived risk associated with mobile banking has a negative impact of mobile banking adoption”. Here the authors suggest that mobile banking adoption means the willingness to use mobile banking rather than using traditional banking. The researcher further describes that the customers distress that their PIN numbers will be lost and their sensitive and confidential banking transaction information may be ended up in wrong hands and those can be tampered by untrusted third parties. The authors suggest that this is an issue related to the trustworthiness of the mobile banking system and mobile banking security has a clear impact on that trustworthiness. Therefore, it is quite clear that mobile banking app security play a vital role in gaining customer trust.

Therefore, this researcher decided to find out whether the reluctance to use mobile banking applications among Sri Lankan banking customers has something to do with trust they have over the mobile banking applications introduced by Sri Lankan banks. As a result, this researcher thought of investigate whether the banking customers’ perception about mobile banking applications security is significantly related to user trust. Apart from that, there is a gap in empirical knowledge with respect to the relationship between the level of security of mobile banking applications to the trust of the users of mobile banking applications. When it comes to the Sri Lankan context, the gap in empirical knowledge about the above factor is very obvious. Therefore, this researcher decided to make a contribution to fill this gap in empirical knowledge with respect to security of mobile banking applications and user trust specially in Sri Lankan context. Thus the problem discussed in this research study is as follows.

What are the perceived degrees of security of the mobile banking applications and user trust;

Do those perceptions relate?

1.3 Research Questions

1. What is the degree of security of mobile banking applications perceived by the users of mobile banking applications?
2. What is the degree of trust of mobile banking applications users?
3. Is the perception of the users of mobile banking applications regarding the degree of security of mobile banking applications significantly related to user trust?
4. What is the most important trust element for mobile banking applications users?
5. What is the most important existing security feature available in current mobile banking applications as perceived by the users?
6. What are security features that can be added to enhance security of mobile banking applications?

1.4 Research Objectives

1. To investigate the degree of security of mobile banking applications perceived by the users of mobile banking applications
2. To investigate the degree of trust of mobile banking applications users.
3. To investigate whether the perception of the users of mobile banking applications regarding the degree of security of mobile banking applications significantly related to user trust.
4. To investigate the most important trust element for mobile banking applications users.
5. To investigate the most important existing security feature available in current mobile banking applications as perceived by the users
6. To investigate security features that can be added to enhance security of mobile banking applications

1.5 Hypothesis

The research is actually quantitative research and the following hypothesis was constructed in order to achieve the research objectives as discussed previously.

Hypothesis 01

H0: There is no relationship between perceived degree of security of mobile banking applications and user trust.

H1: There is a relationship between perceived degree of security of mobile banking applications and user trust.

1.6 Sampling Design

This research was done based on a sample which consist of 220 personnel who are employed in executive category in private and public sector who were selected on a simple random sampling basis from a population of mobile banking applications users in Sri Lanka.

This research is a cross sectional study and data collection was done from the sample over a period of two weeks. The data of the chosen sample was collected deploying the questionnaire method. The questionnaires were administrated using internal contacts of the researcher with the private and public sector executive grade employees.

1.7 Data Analysis

The data regarding the variables that were collected through the questionnaires were codified, quantified, analyzed and evaluated using the SPSS statistical software package. Correlation analysis was deployed to test hypothesis.

1.8 Significance of The Study

The research deals with how level of security of the mobile banking applications available in Sri Lanka affect the trust of the users of such applications. It is well known that mobile banking is one of the most popular modern technology-based innovations that has

contributed a lot for the development of the banking sector. As a result of the dynamic and fast-moving business environment and busy life styles of people, there is no doubt that lots of people are shifting from traditional over the counter banking to mobile banking. With the rapid development in smart devices industry, now mobile banking is at your fingertips and it is much more convenient to perform banking transactions at present. Although mobile banking done through mobile applications available in smart phones is very much popular in today's context, there are some concerns about mobile banking applications as well. Available literature shows that security of the mobile banking applications is the most prominent concern. Users of such applications are very keen about the security of their confidential banking information when they perform mobile banking transactions. Apart from that, according to past research, security is the main reason why most of the people still have kind of reluctance towards using mobile banking applications. Therefore, mobile banking customers expect their service providing banks to ensure safety and security of their bank account information and banking transactions information in mobile banking. In addition to that, mobile banking has become very beneficial for banks as well. Mobile banking provide convenience, cost effectiveness and time saving advantages for banks. Therefore, banks are also promoting mobile banking applications and encourage their customers to use those applications rather than coming to banks and do over the counter manual transactions. In order to promote mobile banking among the customers, today it has become necessary for the banks to ensure proper security in the mobile banking applications they provide. Banks also very keen on developing mobile banking applications with thorough security which has effective ways and means to safeguard the confidential information of their customers. Through the knowledge generated from this research, banks can get a much clear understanding on how the levels of security of the mobile banking applications that they have provided for their customers have impact on trust of their customers.

Apart from that, through this research banks will be able to identify the most important security aspects that current users of their mobile banking applications value most. It will be beneficial for the banks to enhance those aspects and retain their loyal customers for the future as well. On the other hand, through this research, banks will be able to understand the most anticipated security features by the customers. It will be beneficial for the banks

to plan their future developments for their mobile banking applications. Finally, through this research banks get the opportunity to identify the trust elements that customers expect and value most. It will be beneficial for the banks to use it for their applications promotions to retain the current customers and attract future customers. Knowledge generated through this research can be used to formulate strategies regarding mobile banking applications security. In Sri Lankan context, research in this area is very less and this research enables the bankers to look at the mobile banking applications security in a Sri Lankan perspective.

On the other hand, the body of knowledge in banking related research in Sri Lanka will be enhanced through this research study. The research subsidizes to fill the prevailing empirical knowledge gap about the security of the mobile banking applications available in Sri Lanka and trust of the mobile banking customers. Banks and mobile application builders are provided with useful information about the insights of mobile banking applications security and trust of mobile banking customers by this research.

CHAPTER 2

2 Literature Review

In this chapter, researcher attempts to summarize and review what does the existing body of knowledge presents with respect to mobile banking applications security and trust of such applications users.

2.1 A Critical Overview

Mobile banking can be identified as one of the most productive technological innovations of this era. Mobile banking has brought much convenience to the people who are busy with their complicated lifestyles by making all the essential banking transactions available at your fingertips. Revolutionary development in the mobile devices and telecommunication sector has helped a great deal to the enhancement of mobile banking.

Kim, et al.,(2009) describe which as a result of dominance of mobile devices such as mobile tabs, mobile phones and wireless communication networks with Android or IOS supported devices are increasingly involved in financial services and mobile banking is the form of it. The authors further add that “compared to traditional phone banking and tele banking which offer limited number of services, mobile banking is evolving into a rich platform for automated banking and other financial services”. Presenting a quite broader dimension for mobile banking concept Sun et al (2017)describe that mobile banking is basically “an integration of electronic money and mobile communication services”. Explaining it further the researchers point out that this particular integration is performed via the cooperation of multi platform and multi industry between mobile telecommunication services providers and banks.

At present, mobile banking activities are basically performed through a mobile phone application developed in Android or IOS operating systems. Chen, et al., (2018) categorize mobile banking applications as “FinTech” mechanism rather than a “TechFin” mechanism. Discussing about the concept of “FinTech”, the authors state that it is referred to as “Financial Technology” and it can be defined as a modern industry where advanced technologies are functional in financial services and it helps the companies to properly

manage the financial side of the businesses. The authors introduce mobile banking applications naming them as one of the most famous present-day FinTechs and those have been largely utilized by banks to provide various financial services such as bill payments, money transfer and balance checking. Mobile banking done through mobile device applications has derived many advantages to different parties. Summarizing those benefits Nyamtiga, et al., (2013) state that banking done through mobile applications of smart devices offer easy access to customers for their financial possessions comfortably and timely while enabling the service providers to produce extra income.

Although mobile banking performed through applications available in smart devices bring out so many advantages to various parties, there are some concerns as well associated with those platforms. One such issue of paramount importance can be identified as the concerns arising based on the level of security of the transactions done through such applications. Referring to a recent large-scale study Chen, et al., (2018) state that financial services like mobile banking applications are not that secure. The authors further state that they have built an automated security analysis tool known as “Ausera” and 693 mobile banking applications were assessed across over 80 countries. This survey has divulged 2157 vulnerabilities. Many of those could cause grave sensitive data leakage such as PIN, user name and passwords. Therefore, the users emphasize that security of FinTech such as mobile banking applications is very important and crucial for the interest of all the stakeholders.

Therefore, in this literature survey, the researcher attempts to lay a strong theoretical foundation for this research study by analyzing what existing body of knowledge has to offer for the context of this study. Here, the researcher is going to give a broader understanding about the concepts of mobile banking, mobile banking applications, security of mobile banking, pros and cons of mobile banking and its importance and how security of mobile banking applications have impact on trust of the users of such applications.

2.2 History And Origins of The Concept of Mobile Banking

Many researchers have made their attempts to bring out how mobile banking concept was originated and the history of mobile banking. “The history of the mobile banking sector began with the use of Interactive Voice Response (IVR) which is an automated telephony

system that interacts with its callers, gathers relevant information and routes calls to the appropriate destinations” (Alafeef, Singh, & Ahmad, 2011). According to the authors, banking sector used this system to provide various services to its clients. Referring to Laukkanen (2007) the authors further describe that later emergence of bank-based SMS services emerged enabling clients to request the services of a bank by sending text messages. Afterwards, mobile banking sector focused on the Wireless Application Protocol (WAP) based services.

Forwarding some further clarifications to the expressions of the above authors, Pandey (2019) state that initial mobile banking service which used Short Message Service was known as SMS banking. According to the author, in 1999 initially European commercial banks started introducing mobile banking to their customers using Wireless Application Protocol (WAP) platform with the introduction of WAP technology into mobile devices. The author further describe that before 2010, mobile banking was mainly performed by the means of mobile web or SMS banking. In 2011, the first totally functioning banking application was launched and it was available only in Apple IOS devices. Sooner it was found available for Android and Blackberry devices also. According to the author, during the first six months of introduction of this application was signed up by more than one million users and more than one billion funds were transferred using this application.

2.3 A Definitional Approach For Mobile Banking

Research on various aspects of mobile banking has been increased in the recent years as a result of the popularity of mobile banking and the role it has played for a revolutionary development in banking sector. In those researchs and publications, different authors and researchers have defined the concept of mobile banking in different ways.

In order to begin with, the researcher would like to move towards quite an old and basic definition for the concept of mobile banking. Barnes & Corbit(2003)presents such kind of definition and they state that “mobile banking can be defined as a channel whereby the customer interacts with a bank via a mobile device such as a mobile phone or personal digital assistance”. Here the authors argue that the emphasis here is strictly on data communication and mobile banking does not include telephone banking. Bringing some further dimensions, refering to Luakkanen and Passanen (2008), Akturan & Tezcan (2011)

argue that “mobile banking can be seen as a subset of electronic banking and an extension of internet banking with its own unique characteristics”. Mobile banking means the use of smart mobile devices to perform online banking transactions while staying away from your personal computer such as checking account balances, fund transfers, bill payments and locating teller machines (Tracy P, 2020). Bringing further explanations to this, Thiwari and Bus (2007) explain that mobile banking is a provision “of mobile and bank services by using telecommunication device, the services may include keep in contact with bank to administer account and access customized information”.

Making the definition of mobile banking much broader, Pousttchi & Schurig (2013) present much broader definition that “it is a type of execution of financial services in the course of which the customer uses mobile communication techniques through mobile devices”. Here the authors have put their attention to describe what mobile devices are as well. According to the authors mobile devices are such devices which are typically mobile, easily transportable and use of such are typically stationary.

Introducing another dimension to the concept of mobile banking Elkhodr, et al (2012) suggest that mobile banking could be measured as one of the mobile commerce applications. According to the authors the speedy developments in M-Commerce applications has reformed traditional banking services to an industry of mobile banking. Adding some more facts into this and referring to Mohammadi (2015), Emmanuel et al (2016) state that mobile banking is a facet of M-Commerce and a natural development of E-Banking and it has added some sort of mobility in bank service conveyance to bank customers.

2.4 Mobile Banking Services

Taking all the above-mentioned definitions into consideration, it is obvious that mobile banking is a way of performing banking transaction by means of mobile device applications. There are a lot of banking transactions which have been made possible through mobile applications with the development of technology of mobile devices and mobile banking. Anyasi & Otubu (2009) point out a list of banking transactions which can be executed using mobile banking.

2.4.1 Information about accounts:

- Account history checking and mini statement generating
- Sending alerts about account activities
- Fixed term deposits monitoring
- Providing loan statements
- Providing card statements
- Statements about mutual funds
- Management of insurance policy
- Management of pension schemes
- Statements and status regarding checks and stop payments

2.4.2 Fund Transfers and Bill Payments:

- Fund transfers (domestic and international)
- Handling of micro level payments
- Recharging mobile SIM cards
- Processing commercial payments
- Processing bill payments
- Processing peer to peer payments

2.4.3 Services on Investment:

- Services about investment portfolio management
- Stock quotes generated real time
- Notifications regarding securities prices

2.4.4 Support Services:

- Status regarding credit requests and mortgages
- Processing requests for credit cards and cheques
- Data messages and e mail exchanging

2.4.5 Contented Services:

- Weather updates and news related services
- Loyalty offers
- Location based services

2.5 Platforms of Mobile Banking

Mobile banking can be done based on different types of platforms. In early days, customers had the opportunity to check account balances and perform bill payments via mobile phones through the use of Global Standard for Mobile (GSM) networks (Barnes & Corbit, 2003). The authors further explain that at current mobile banking applications have relied heavily on the progress of wireless electronic amenities. Examples of these modern mobile banking platforms include;

2.5.1 WAP Banking

WAP or Wireless Application Protocol is “a universal standard for bringing internet-based content and advanced value-added services to wireless devices such as phones and PDAs” (Barnes & Corbit, 2003). The authors further explain that “WAP sites are hosted on web servers and use the same transmission protocol as web sites. Here, a wireless device will send a request for information to a server and the server responds with sending packets of data which will be displayed through browsers. Mobile banking was one of the first transactions enabled services to be provided using this WAP platform”.

2.5.2 SMS Banking

“SMS allows text messages to be sent to and from mobile devices via store and forward system” (Barnes & Corbit, 2003). “This platform is based on simple input/output interaction where the bank’s system will text or read to you an inquiry for which the user

has to respond with an input. The system provides a response to each step of this process with a corresponding output based on the user requests” (Johnson et al, 2012).

2.5.3 Standalone Applications

“This requires users to download apps, which are extremely user friendly and allow banks to customize and brand the pages to their liking. This approach is widely regarded as the future of mobile banking” (Johnson et al, 2012). With the revolutionary developments in the sector of smart devices, there are various mobile applications developed using computer software technologies available at a click in the play store or app store in today’s mobile devices.

Kathryn V (2010) brings out several aspects of mobile banking. According to the author there are five aspects of mobile banking experience as;

1. Mobile payments
2. Mobile check processing
3. SMS banking
4. Mobile banking apps
5. General banking through the mobile web

2.6 Mobile Banking Applications

Various platforms that mobile banking is performed were discussed above. Out of these several aspects of mobile banking, this particular study focuses on mobile banking apps and their security. When smart phones came to the stage from cell phones, and the extent and capabilities of mobile equipment improved, mobile banking effectiveness also enhanced. Mobile banking applications introduced by banks that lodged more types of mobile phones, instead users of smart phones and advanced applications enabled mobile banking the improvement which made it a secure and practical choice. Customers favored the easier navigation and improved graphics and images given by these apps that are technically advanced and updated.

It is now quite evident that mobile phone application is the platform that is used in almost all the occasions today. Providing a definition for what a mobile application means, (Henry Muccini, 2010) state that mobile application is an application determined by inputs of the user, operates on a mobile device and producing context based outputs. Therefore, applications dedicated to mobile banking can be identified as a mobile application supplied by a bank or financial organization which allows banking transactions to be performed online.

Bringing up a quite comprehensive definition for mobile banking applications, Alafeef, Singh, & Ahmad (2011) describe that mobile banking applications are “type of execution of financial services in the course of which within an electronic procedure the clients use mobile communication techniques in conjunction with mobile devices”. These mobile banking applications provide electronic platform for its users to perform banking activities such as bill payments and fund transfers. here the authors indicate that mobile banking application is generally an electronic platform which facilitates banking transactions.

“Banks, through mobile banking applications, provide a combination of payments, banking, real time two way data transmission and access to financial information and services” (Akturan & Tezcan, 2011). Here, the authors highlight about the services rendered by mobile banking applications. The authors further argue that at present mobile banking applications are growing as a new marketing channel for banks and it can be considered as an important aspect of development strategies for both the banking and mobile device industries.

At present, use of smart devices such as smart mobile phones, tabs and smart lap tops has become very popular and those have been recognized an essential element of day to day lives of people. There are various mobile applications included in those devices which enable the users to perform different types of activities through the operating system. Banks have used this to a good effect and introduced mobile banking applications. Those can be downloaded directly from play store or app store based on the operating system. At present not only in developed countries, Sri Lankan banks also have introduced this facility to their customers.

2.6.1 Advantages Of Mobile Banking

There is no doubt that mobile banking is one of the rapidly growing sectors in e-commerce field. It has become so popular among the banking customers not only globally but also in Sri Lanka as well. The very reason for all this rapid growth and popularity is the advantages derived through mobile banking. Many researchers have made attempts to figure out and present about the advantages derived through mobile banking.

In order to begin with, referring to Ha el al (2012) and Garrett (2011), Lee at al (2013) designated that the advantages of utilizing mobile banking include,

- Omnipresence
- Proximity
- Localization
- Rapid connectivity
- Hands-on functionality

Adding more facts to this, the authors further mention that through mobile banking, the operating costs can be cut and make it a competitive strategy for financial institutions and banks.

Bringing out quite broader facts with respect to advantages of mobile banking, Manali (2014) explains some advantages of mobile banking may include,

- Volume of Sales Enhanced

A satisfactory status of an organization's logistical sizes may help produce additional orders. Mobile Banking could subsidize to achieve this objective by providing ubiquitous access to banking services.

- Increasing Customer Satisfaction

Mobile Banking could help enhance the customer satisfaction via rationalization of business processes to enhance efficiency, much attention and better consulting for

customers due to automation of routine processes, innovative ubiquitous services customized for individual favorites and present geographic location of the customer provide value-added to the customer while the collected data can be used to create customer profiles. Increased customer satisfaction can help reduce the customer abrasion rate.

- **Source of Revenue**

Mobile Banking could also help as a source of revenue. Mobile services can be supplied on a quality basis. The price should be reasonable enough so that customers are keen to pay them but at the same time they should be from a monetary point of view higher than the costs generated by the bank. Additional revenues can be generated by submission of innovative, premium services to existing customers and attracting potential customers by offering innovative services.

- **Distribution Costs Reduction**

As a result of increased competition, a distribution channel must organize business processes productively in order to reduce distribution costs. This pressure can be dealt with rationalizing organizational structures to increase efficiency and effectiveness. Mobile Banking could help to achieve this objective since the manual collection, processing, dissemination and archiving of data by bank employees in branch offices is substituted, as in the online based banking through automated processes.

2.6.2 Disadvantages Associated with Mobile Banking

Apart from the above-mentioned advantages of mobile banking, arguments have been arised about the possible disadvantages of mobile banking as well. Chandran (2014) presents some of them as below;

- Users of mobile banking face the risk of receiving fake SMS messages and scams.
- Mobile device losses often means that hackers and other criminals can gain access to one's mobile banking PIN and other sensitive information.

- Regular mobile banking users can gather large charges from banks over time.
- The threat of hackers accessing one's private and confidential information and sensitive banking transactions is possible.
- Mobile banking applications require an internet connection to function. Therefore people live in a rural areas or people who have troubles with their internet connection will not be able to access their bank accounts through mobile banking applications.
- Several phones are still not well suited for antivirus software. Some mobile phones do not possess ordinary antivirus protection, even if they have the ability to browse the web.

2.7 Security Of Mobile Banking

When possible, strategic challenges related to mobile banking is concerned, it can be recognized that one of the main challenges is the security of the applications designed for mobile banking. It is much evident in above mentioned disadvantages as well. Findings of the research carried out by Kaya (2013) recognise one factor as a strong reason for the users of mobile banking applications not to assume mobile banking and it is their concerns for security. The same author highlights that one of the main reasons for lower adoption for mobile banking and use of mobile banking applications is the concerns of security. Referring to a recent large-scale study Chen, et al., (2018) state that financial services like mobile banking applications are not that secure. The authors further state that they have built an automated security analysis method known as "Ausera" and evaluated 693 mobile banking applications across more than 80 countries. This survey has exposed 2157 defenselessness, most of those could cause considerable sensitive data leakage such as passwords, PINs and user name. Therefore, it has become a critical area of importance. Many scholars, researchers and experts of the field have paid much attention to it.

According to Rouse, M (2013), "Mobile app security is the extent of protection that mobile device applications (apps) have from malware and the activities of crackers and other criminals. The term can also refer to various technologies and production practices that

minimize the risk of exploits to mobile devices through their apps”. Unfolding some further aspects about mobile banking security FraudWatch International (2019) suggests that “Mobile banking app security is the measure and means of defending mobile device apps from digital fraud in the form of malware, hacking, and other criminal manipulation”.

Mobile banking applications developers and banks have designed and deployed various kinds of security controls for mobile banking applications in order to ensure security of the applications. According to Bucko (2016), limits of incorrect logins can be identified as one of the important security control measures adopted by the banks in mobile banking applications. The researcher further explains that a user may be allowed to insert incorrect login elements maximum 3-5 times in a row. Bringing some more aspects to the concept of security controls, the same author argues that automatic check out is also a productive security related control methods adopted by mobile banking applications. According to the researcher, it is a protective mechanism in case of long inactivity. The author ultimately suggests that trust of the mobile banking applications users can be gained effectively when banks encompasses this type of security features to the applications.

Considering all those definitions about mobile banking application security, it can be summarized that mobile banking applications security refers to those mechanisms deployed by the developers of mobile banking applications using computer programming languages to protect the application from threats such as malware, hacking, activities of crackers and hackers in order to safeguard the information and privacy of the users of such applications.

2.7.1 Types Of Security Related Threats for Mobile Banking

Many researchers have made attempts to find out what may the possible threats be for mobile banking applications. Bringing out some basic level set of threats Bojjagani & Sastry (2016) state three types of threat scenarios associated with mobile banking applications.

- Bank data earned by untrusted parties: Personnel who are not authorized could obtain the bank and banking transactions information belonging to a customer
- Bank data tampering: Adverse tampering or alteration of banking data of an individual customer by means of replay of performs or hacker attacks in the network and communication media.
- Risk of customers choosing wrong bank app: At this stage, banking customer selects a fake mobile banking application from play store or app store. Then it is downloaded to the mobile device and give valid identifications to a party not trusted.

These authors further add that the above-mentioned types of threat scenarios characterize the abuse of security features such as confidentiality, integrity of data, authentication, authorization and non-repudiation.

Apart from that the authors present a diagram showing a distinctive threat situation for mobile banking applications as shown below. According to the authors, the heart signs in the diagram represent fine grained banking data.

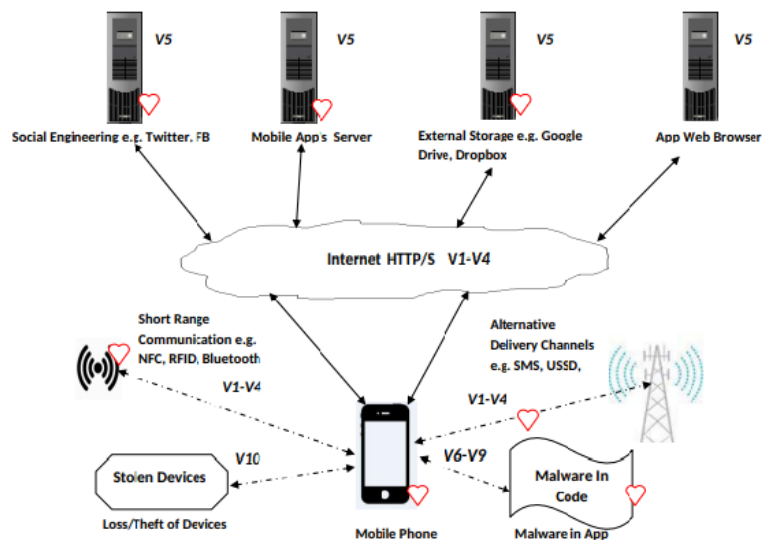


Figure 2.1: A typical threat scenario for mobile banking apps

Source: Bojjagani & Sastry (2016)

Adding some more to the facts about what affect the security of mobile banking, Kaya (2013) state that the following can be considered as major threats for mobile banking applications.

2.7.1.1 Rootkits

Rootkits can be considered as malware that make adverse effect on data of mobile banking applications by infecting the operating system. For example, rootkits can be used to mount Trojan horses and deactivate firewalls and disable virus scanners. Following are a list of vulnerabilities that a rootkit can exploit with respect to mobile banking applications when installed in a smart device.

- Financial damage by sending text messages to first-class numbers in such events where SMS is used for mobile banking transactions
- Access to passwords and other information that is typed or saved
- Record voice conversations which expose sensitive information
- Denial of service via attacks using SMS or Bluetooth
- Denial of service via battery exhaustion
- Attacks of network based and web based

Those are performed in mobile browser where malicious web sites trigger the attack if the mobile runs a vulnerable version of the operating system. In such event, attacking web site send malicious amount of data to the browser of web. Then this web browser runs nasty instructions sent by the hacker or attacker which allow the attacker to access confidential information.

2.7.1.2 Social Engineering Attacks

These attacks try to make the user disclose information often by means of email or SMS which directs user to a web site that seems like legitimate but fake and it has intention to collect banking information of the users.

2.7.1.3 Resource Abuse Attacks

This type of attacks misuses the network. This is done usually by sending spam emails and using cooperated equipment to launch rejection of service attacks on third party web sites or data network.

2.7.1.4 Data Loss

Data losses happen when an attacker removes sensitive data and information from a safeguarded device or network without proper authorization.

2.7.1.5 Data Integrity Threats

In this kind of a threat, the attacker attempts to make the data corrupted or modified without permission from the owner of those data.

2.8 User Trust

There are many researches about the facts which affect the trust of the users of mobile banking applications. Many of them have been about the role of trust for the mobile banking adoption. Many researchers argue that initial trust and/or trust as a hole are one of the key components which determine mobile banking adoption which can be alternatively introduced as willingness to use mobile banking instead of traditional over the counter banking or somewhat modern internet banking.

“Trust is a psychological expectation that a trusted party will not behave opportunistically” Kim et al. (2009). Those authors further explain the trust concept referring to Mayer et al. (1995) that “trust represents the willingness of one party to be vulnerable to the actions of other parties”. Apart from that referring to Whitener et al. (1998) the authors describe that “it is assumed in a trust relationship that the trusted party will behave compassionately and there is a certain level of dependency between the tuster and trustee”. As far as these definitions are concerned interdependency and risks are the essential situations of trust and it is very conducive to psychological phenomenons such as willingness, attitudes, perceived probability and expectations.

On the other hand, when attention is paid to the dimensions of trust, Lee & Chung (2009) state that “trust has two dimensions as credibility and benevolence. Clarifying these two dimensions the authors add that credibility is the belief that business partners would fulfill

their roles reliably and effectively where benevolence refers to the belief that business partners have the necessary motivation and intent to provide benefits”. Referring to Ba and Pavlou (2002) and McKnight et al. (2002) the authors highlight that “trust is a very important factor in mobile banking because mobile banking happens online and it involves money”. Adding further clarifications, the authors go on describing that an important role is played by trust in the technology acceptance and the readiness for online purchases. In addition, Kaya (2013) describe that “mobile banking trust can be divided into two categories as initial trust and continuous trust. Both of these aspects are affected by the factors related to mobile vendor and technology”.

“Trust provides a guarantee that mobile banking users buy mobile banking services provided, they also feel that the use of mobile banking is guaranteed and will have a better sense of experience “Sun et al. (2017). It is now quite evident that trust is a much essential factor in mobile banking. Here basically trust is meant by the level of trust of the mobile banking facilities of applications users. Many researchers have made their attempts to figure out what are the factors that has a considerable impact on trust of the customers of mobile banking. Findings of the research carried out by Kaya (2013) recognise one factor as a strong reason for the users of mobile banking applications not to adopt mobile banking and it is their concerns for security. The same author highlights that one of the main reasons for lower adoption for mobile banking and use of mobile banking applications is the concerns of security. Apart from that in their research findings Kim et al (2009) point out which “relative benefits, propensity to trust and security assurances had a significant effect on initial trust of mobile banking”. In addition, findings of the study carried out by Jabri & Sohail (2012) shows that perceived risk associated with mobile banking has a negative influence of mobile banking adoption. Here the authors suggest that mobile banking adoption means the willingness to use mobile banking rather than using traditional banking. The researcher further describes that the customers distress that their PIN may be lost and their sensitive and confidential banking transaction information may be ended up in wrong hands and those can be tampered by untrusted third parties. The authors suggest that this is an issue related to trustworthiness of the mobile banking system and security of mobile banking has a clear impact on that trustworthiness. Therefore, it is quite evident that mobile banking app security play a vital role in gaining customer trust.

Though there are some research-based literatures are available in global context with respect to mobile phone applications security and how it may be affected to customer trust, there is a serious deficit in empirical evidence in Sri Lankan context for this area. Summarizing mobile banking trust related literature Kaya (2013) explains that “similar to online transactions, mobile banking also involves great ambiguity and risk. Thus, trust is critical to assisting mobile user behavior. However, compared to the lavish research on online trust, there exists less research on mobile trust”. Therefore, through this study, the researcher attempts to contribute in a productive way to fill this gap of empirical evidence in mobile banking application security and how user trust is affected by that.

CHAPTER 3

3 Conceptualization, Operationalization and Methodology

This section converses on the theoretical framework of the research, working definitions of the variables of the theoretical or conceptual framework, operationalization of the research and methodology used which includes nature of the study, type of investigation, unit of analysis, population and sample, data collection methods and data analysis methods.

3.1 Conceptualization

3.1.1 Theoretical Framework

Theoretical framework concept can be described as “logically developed, described and elaborated network of associations among the variables deemed relevant to the problem situation and identified through such processes as interviews, observations and literature review” (Sekaran & Bougie, 2011). Therefore, below displayed theoretical framework was erected for this research study according to the problem statement, objectives of the research and literature review.

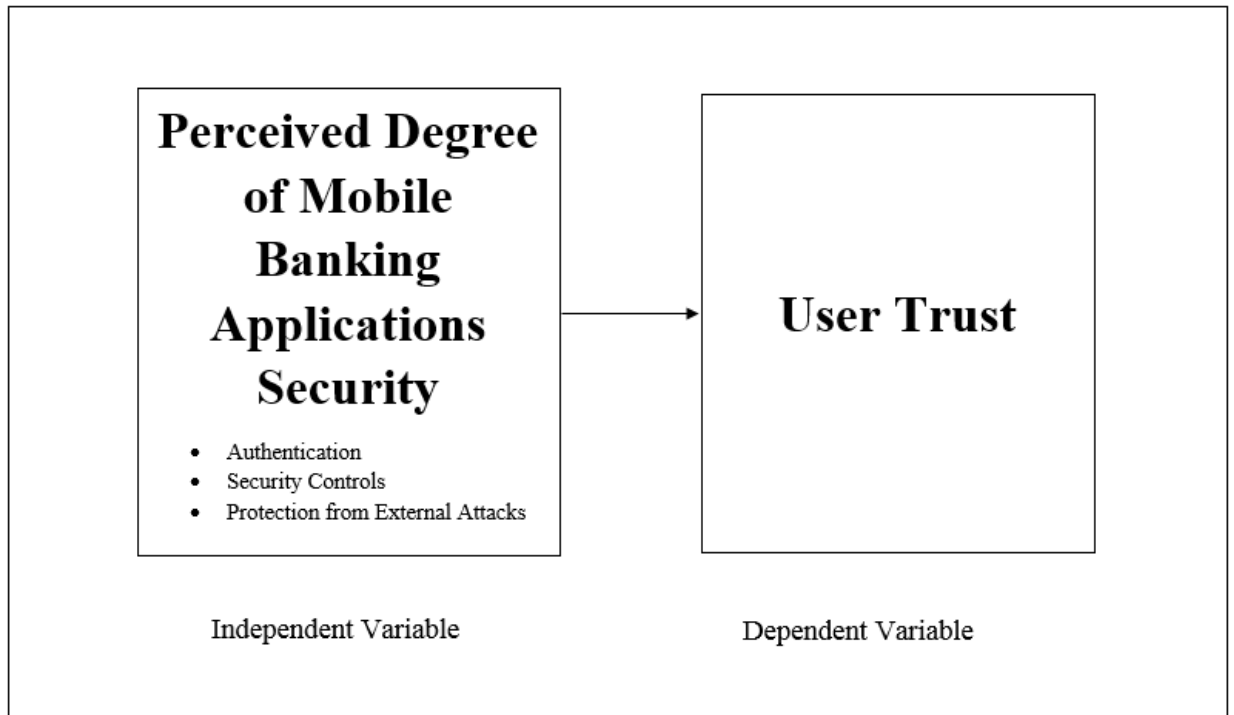


Figure 3.1: Theoretical Framework

According to the schematic diagram shown in the above figure, trust of mobile banking applications users is considered as the dependent variable. This researcher observed that most of the banking customers in Sri Lanka are still very reluctant to use mobile banking applications although mobile banking applications enable the users to conveniently perform banking transactions without wasting time in the counters. Specially in a pandemic period like this where people are strictly advised to avoid large gatherings, this researcher still saw long queues in front of the banks. Although banks have introduced mobile banking applications and people own smart devices, people rarely use mobile banking applications. As per the observations made by the researcher and arguments made by various researchers in this area of interest, this is basically due to a trust issue they have with the mobile banking applications. Perceived degree of security of mobile banking applications especially related to Sri Lanka is considered as the independent variable in this research theoretical framework. According to the prevailing literature as described in chapter two above, many researchers have argued that this aspect is the most influential aspect for the

trust of mobile banking applications users. Therefore, in this research as well, the researcher argues that security is the most prominent concern and influential factor for trust of the users of such applications specially in the Sri Lankan context where technology is still at under developed stage. According to literature, authentication, security controls and protection from external attacks are key features of mobile banking application security. As described in literature review, many researchers have argued that these elements of mobile banking applications security are influential in gaining user trust.

3.1.1.1 Working Definitions of the Variables

3.1.1.1.1 Security Of Mobile Banking Applications

When possible, strategic challenges related to mobile banking is concerned, it can be identified that one of the major challenges is the security of mobile banking applications. Findings of the research carried out by Kaya (2013) recognise one factor as a strong reason for the users of mobile banking applications not to adopt mobile banking and it is their concerns for security. Referring to a recent large-scale study Chen, et al., (2018) state that financial services like mobile banking applications are not that secure. Therefore, it has become a critical area of importance. Many scholars, researchers and experts of the field have paid much attention to it. Unfolding some further aspects about mobile banking security FraudWatch International (2019) suggests that “Mobile banking app security is the measure and means of defending mobile device apps from digital fraud in the form of malware, hacking, and other criminal manipulation”.

For the purpose of this research, the researcher selected the definition presented by Rouse, M (2013) that “Mobile app security is the extent of protection that mobile device applications (apps) have from malware and the activities of crackers and other criminals as the base definition and the researcher wishes to add that mobile banking applications security refers to those mechanisms deployed by the developers of mobile banking applications using computer programming languages to protect the application from threats such as malware, hacking, activities of crackers and hackers in order to safeguard the information and privacy of the users of such applications”.

3.1.1.1.2 Trust of The Mobile Banking Users

There are many researches about the facts which affect the trust of the users of mobile banking applications. Most of them have been about the role of trust for the mobile banking adoption. Many researchers argue that initial trust and/or trust as a whole are one of the key components which determine mobile banking adoption which can be alternatively introduced as willingness to use mobile banking instead of traditional over the counter banking or somewhat modern internet banking.

“Trust is a psychological expectation that a trusted party will not behave opportunistically” Kim et al. (2009). Whitener et al. (1998) the authors describe that “it is assumed in a trust relationship that the trusted party will behave compassionately and there is a certain level of dependency between the trustor and trustee”.

The researcher intends to use the definition presented by Mayer et al. (1995) that “trust represents the willingness of one party to be vulnerable to the actions of other parties as the working definition for the concept of trust”.

3.1.2 Hypothesis

In order to confirm the conjectured relationships, the following hypothesis were derived based on the reviewed literature and conceptual framework.

3.1.2.1 Hypothesis 1

Many researchers have made their attempts to figure out what are the factors that has a considerable impact on trust of the users of mobile banking. Findings of the research carried out by Kaya (2013) recognise one factor as a strong reason for the users of mobile banking applications not to adopt mobile banking and it is their concerns for security. The same author highlights that one of the main reasons for lower adoption for mobile banking and use of mobile banking applications is the concerns of security. Apart from that in their research findings Kim et al (2009) point out that “relative benefits, propensity to trust and security assurances had a significant effect on initial trust of mobile banking”. On the other hand, findings of the study carried out by Jabri & Sohail (2012) shows that perceived risk associated with mobile banking has a negative impact of mobile banking adoption. Here

the authors suggest that mobile banking adoption means the willingness to use mobile banking rather than using traditional banking. The researcher further describes that the customers fear that their PIN codes may get lost and their sensitive and confidential banking transaction information may be ended up in wrong hands and those can be tampered by untrusted third parties. The authors suggest that this is an issue related to the trustworthiness of the mobile banking system and mobile banking security has a clear impact on that trustworthiness. According to Kaya (2013), “security related authentication can be identified as one of the crucial elements for mobile banking adoption of the banking customers”. Adding more clarifications to this, Bojjagani & Sastry (2016) explain that “one of the main reasons for lower mobile banking adoption is that the perceived vulnerabilities of the users that unauthorized parties will access the mobile networks and the important financial information of the customers will go to unwanted hands”. Therefore, it can be argued that this is also a matter of proper authentication. Mobile banking applications developers and banks have designed and deployed various kinds of security controls for mobile banking applications in order to ensure security of the applications. According to Bucko (2016), limits of incorrect logins can be identified as one of the important security control measures adopted by the banks in mobile banking applications. The researcher further explains that a user may be allowed to insert incorrect login elements maximum 3-5 times in a row. Bringing some more aspects to the concept of security controls, the same author argues that automatic check out is also a productive security related control methods adopted by mobile banking applications. According to the researcher, it is a protective mechanism in case of long inactivity. The author ultimately suggests that trust of the mobile banking applications users can be gained effectively when banks encompasses this type of security features to the applications. Apart from that, Chandran (2014) presents that in mobile banking applications there is a threat of hackers accessing your private and confidential information and sensitive bank transactions. The author further argues that it has become one of the main reasons for reluctance to use mobile banking applications. According to the above arguments, it can be hypothesized that;

H0: There is no relationship between perceived degree of security of mobile banking applications and user trust

H1: There is a relationship between perceived degree of security of mobile banking applications and user trust

3.2 Operationalization

3.2.1 Operationalization Of Mobile Banking Applications Security

Mobile banking application users' perceived degree of security of the mobile banking applications was operationalized into three dimensions as authentication, security controls and external attacks. Then every dimension was operationalized into some elements referring to literature as well. Afterwards, question was formulated with respect to the recognized elements. Since three mobile banking applications security elements were considered under the study, seven instruments were developed with respect to the dimensions and elements of mobile banking applications security. Each question was raised on a five-point scale of consensus, consensus, neutrality, disagreement, and consensus. Values of 5,4,3,2 and 1 were given to the responses. The following table summarizes the sources of relevant literature used to construct the instruments.

Table 3-1: Operationalization of security of mobile banking applications

Dimensions and elements	Relevant resources
Authentication	Bojjagani & Sastry, 2016, Kaya, 2013
Security Controls	Chen, et al., 2018, Bucko (2016), Kaya, 2013
External Attacks	Kaya, 2013, Chandran (2014), Rouse, M (2013)

3.2.2 Operationalization Of User Trust

Degree of trust of the users of mobile banking applications regarding the mobile banking applications that are being used operationalized into three dimensions. In deriving these dimensions, the researcher selected the dimensions of trust described by Lee & Chung (2009). When attention is paid to the dimensions of trust, Lee & Chung (2009) state that “trust has two dimensions as credibility and benevolence. Clarifying these two dimensions the authors add that credibility is the belief that business partners would fulfill their roles

reliably and effectively where benevolence refers to the belief that business partners have the necessary motivation and intent to provide benefits”.

Kim, Shin, & Lee (2009) suggest that structural elements and firm reputation play a vital role in determining trust. “Structural assurances in the form of agreements, contracts, regulations, policies, laws, feedback forums, guarantees, escrow services and others enhance initial trust between involved parties in relationship” (Kim, Shin, & Lee, 2009). According to the authors “people’s perception about a service can be affected by institutional indications and their ideas about the reputation which has been conveyed to them formally and informally”. The authors name that element as firm reputation. Ultimately in this research, the trust elements namely credibility, benevalence, structural assurances and firm reputation are considered for operationalization of the dependent variable, user trust.

After that every dimension was operationalized into several elements referring to literature. After that questions were formulated in relation to the recognized elements. As two mobile banking applications security elements were considered under the study, four questions were formulated with regard to the dimensions and elements of mobile banking applications security. Each question item was elicited on a five point scale of strongly agree, agree, moderate, disagree and strongly agree. Values of 5,4,3,2 and 1 were given to the responses.

3.2.3 Operationalization Of Frequency Of Mobile Banking Applications Usage

The variable of age limits of the mobile banking applications users was measured through one direct question. The question contains four levels of frequency of usage as follows;

- Below 30 years
- 31-40 years
- 41-50 years
- Above 50 years

3.2.4 Gender

This variable was measured using one direct question

- Male
- Female

3.3 Methodology

3.3.1 Purpose Of The Study

The purpose of this research is to identify what are the perceived degrees of security of the mobile banking applications available in Sri Lanka and trust of mobile banking applications users and investigate whether those perceptions relate. Apart from that, security elements with respect to mobile banking applications are taken separately and investigations will be done about the relationship that those variables separately have with user trust. Therefore, this research is basically a descriptive study. The study engages hypothesis testing to explain the nature of relationships and establish the differences of the variables identified in the conceptual framework.

3.3.2 Type Of Investigation

This research is mainly a correlational study. The main goal of this research is to outline or demarcate the important variables associated with the research problem of this research. The study was undertaken in the natural environment of the organization with minimal interferences by the researcher with the normal flow of work.

3.3.3 Study Setting And Unit Of Analysis

The study was done in the natural environment where work proceeded normally. None of the variables were controlled and manipulated. Hence this study is not a contrived study. Individual response of the current users of mobile banking applications is concerned for the study. The target users are executive grade employees in both public and private sectors. Hence the unit of analysis of the study is individual.

3.3.4 Methodological Choice

This research relied on survey method since the researcher assumed it to be the most appropriate according to the nature of the study. The survey method is characterized by a

self administrated structured questionnaire which was used to collection of data. Majority of this study is based on primary data and it is the reason why the survey method was found to be more suitable to collect required data due to its comparative advantages in terms of time and cost.

3.3.5 Population

The target population for this study public and private sector executive grade employees who are using mobile banking applications.

3.3.6 Sample

A sample of 220 individuals was used as the sample of this study. The researcher used the simple random sampling technique to select the respondents.

3.3.7 Data Collection Methods

The researcher used structured questionnaire method to collect data from the sample. This research is mainly a cross sectional study and data was collected from the selected sample over a period of three weeks. The questionnaires were administrated through internal contacts of the researcher in reputed private and public sector organizations and later returned to the researcher. All the questionnaires sent were returned after completion of answering yielding a response rate of 100%. The questionnaire consisted of two main parts. The first part was allocated to trap gender and age groups of the respondents. The second part consisted of fifteen instruments to trap the perceived degree of security of mobile banking applications and trust of the users of such applications for their day to day banking purposes.

3.3.8 Data Presentation And Analysis

The data on variables, collected and measured by the questionnaires, had been codified, quantified, analyzed and evaluated using the SPSS. Data is presented in tabular and graphical forms using the techniques available in SPSS. The first part of the analysis is the univariate analysis. In that, frequencies of the variables, mean and standard deviation were used as descriptive statistics. The second part of the analysis is allocated for bivariate analysis. Correlation analysis was deployed to test the hypothesis.

CHAPTER 4

4 Data Presentation and Data Analysis

4.1 Introduction

In this chapter, collected data using the questionnaire method is arranged and analyzed in order to come up with findings and thus derive conclusions. This chapter on data display is divided into two sections;

- Univariate analysis - here, the researcher analyzes one variable at a time and is basically based on descriptive statistics.
- Bivariate analysis - here, the researcher tests the hypothesis mentioned in the previous chapter using correlation analysis.

Data are presented mainly in tabular and graphical form.

4.2 Univariate Analysis

4.2.1 Frequency distribution analysis of respondents by their personal characteristics

The data collected on personal characteristics such as gender and level of education is presented and analyzed as follows.

4.2.1.1 Composition of the sample according to gender

Table 4-1: Gender distribution

		gender			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	149	67.7	67.7	67.7
	Female	71	32.3	32.3	100.0
	Total	220	100.0	100.0	

Source: Survey Data

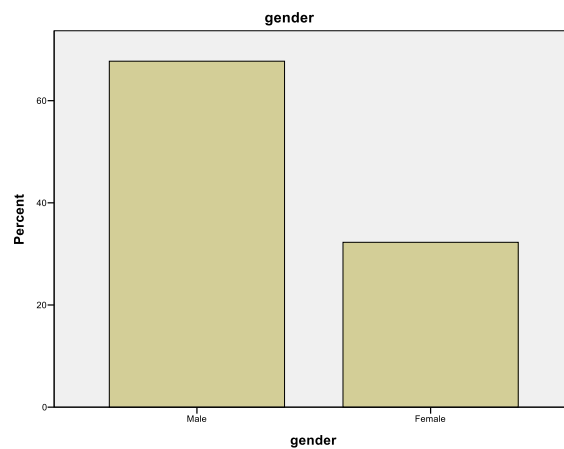


Figure 4.1: Gender distribution

Source: Survey Data

Gender of the respondents of the sample was categorized as male and female. Table 4.1 and figure 4.1 present the gender distribution of the total sample. Male respondents are denoted by No. 1 and female respondents are denoted by No. 2.

According to the table 4.1 and figure 4.1, 149 individuals out of 220 respondents in the sample are male and their percentage is 67.7%. The rest 71 respondents are female and their percentage counts as 32.3%. Therefore, it is quite evident that the use of mobile banking applications is very common among both the genders.

4.2.1.2 Composition of the sample according age groups

Table 4-2: Distribution according to the age groups

		age			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Below 30 Years	5	2.3	2.3	2.3
	31-40 Years	60	27.3	27.3	29.5
	41-50 Years	86	39.1	39.1	68.6
	Above 50 Years	69	31.4	31.4	100.0
	Total	220	100.0	100.0	

Source: Survey Data

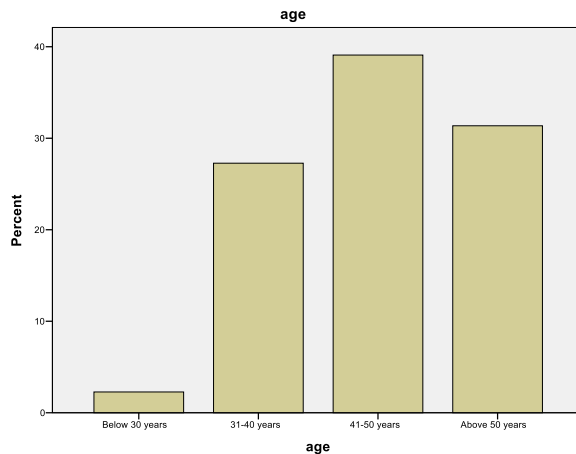


Figure 4.2: Distribution according to the age limits of the users

Source: Survey Data

Age limits of the respondents of the sample was categorized into four categories as;

- Below 30 years
- 31-40 years

- 41-50 years
- Above 50 years

Table 4.2 and figure 4.2 present the employment sector distribution of the total sample.

According to the table 4.2 and figure 4.2, 5 individuals out of 220 respondents in the sample are below 30 years of age and their percentage is 2.3%. Another 60 individuals out of 220 are in the age category of 31-40 marking their percentage as 27.3%. Another 86 individuals out of 220 are from 41-50 age group and their percentage is 39.1%. The rest 69 respondents are above 50 years of age and their percentage counts as 31.4%.

4.2.2 Descriptive statistics

In this section, researcher tries to identify the level of responses given by the sample regarding each independent variable and the dependent variable. According to the conceptual framework, the independent variable of the research is the perceived degree of security of the mobile banking applications and the dependent variable is user trust. Five-point Likert Scale was used in questions to trap these two variables and the scales were weighted as follows;

Standard Value	Weight
Strongly Agree	5
Agree	4
Neutral	3
Disagree	2
Strongly Disagree	1

4.2.2.1 Mean and standard deviation of perceived degree of security of mobile banking applications

Table 4-3: Mean and standard deviation coefficients of perceived degree of security of mobile banking applications

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Mean_sec	220	1.43	5.00	3.9370	.72060
Valid N (listwise)	220				

Source: Survey Data

According to the table 4.3, mean value of the perceived degree of security of mobile banking applications is 3.94. According to this coefficient it can be concluded that it is at above average level close to high level of perceived degree of security of the mobile banking applications.

The standard deviation of perceived degree of security of mobile banking applications is 0.72. Standard deviation shows how much the dispersion of data from mean. Standard deviation of perceived degree security of the mobile banking applications indicates a comparatively higher level of dispersion of the variable.

4.2.2.2 Mean and Standard deviation of user trust

Table 4-4: Mean and Standard Deviation coefficients of user trust

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Mean_trust	220	1.50	5.00	3.8284	.77219
Valid N (listwise)	220				

Source: Survey Data

According to the table 4.4, mean value of user trust is 3.83. According to this coefficient it can be concluded that it is at above average level close to high level of user. The standard deviation of degree of trust of mobile banking applications is 0.77 which indicates a high level of dispersion of the variable.

4.3 Bivariate Analysis

Bivariate analysis includes correlation analysis to test the hypothesis of the study

4.3.1 Correlation analysis

Correlation analysis explains the relationship among to variables. Correlation coefficient indicates the strength and the direction of the relationship can be computes by applying a formula that takes in to consideration the two sets of figures (Sekaran & Bougie, 2011).

Table 4-5: Correlation between perceived degree of security of mobile banking applications and user trust

Correlations		Mean_sec	Mean_trust
Mean_sec	Pearson Correlation	1	.854 **
	Sig. (2-tailed)		.000
	N	220	220
Mean_trust	Pearson Correlation	.854 **	1
	Sig. (2-tailed)	.000	
	N	220	220

** . Correlation is significant at the 0.01 level (2-tailed).

Source: Survey Data

The hypothesis was formulated to investigate the relationship between perceived degree of security of the mobile banking applications and user trust. In order to test the hypothesis, the suitable statistical test was Pearson Product Correlation Coefficient. Since the alternative hypothesis is non directional, two tailed test was used.

According to the table 4.5, the Pearson Correlation Coefficient is 0.854 which is positive. This indicates that there is a strong positive correlation between perceived degree of security of mobile banking applications and user trust. In order to find out whether the correlation coefficient derived is statistically significant, significance test was carried out. As the significant value is less than 0.01 the correlation coefficient is statistically significant. Therefore, there is statistical evidence to claim that there is a relationship between perceived degree of security of mobile banking applications and user trust.

Ranking of the trust elements

Table 4-6: Ranking of credibility

Credibility		Frequency	Percent
Valid	1st choice	56	25.5
	2nd choice	118	53.6
	3rd choice	44	20.0
	4th choice	2	.9
	Total	220	100.0

Source: Survey Data

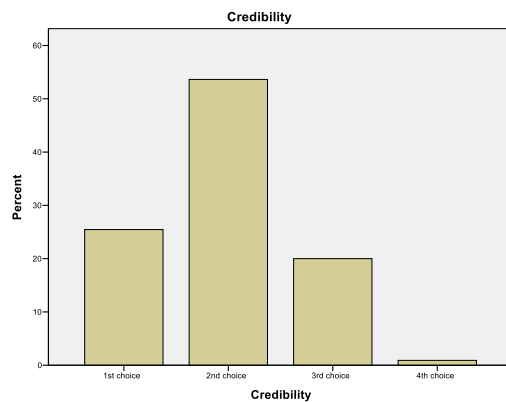


Figure 4.3: Ranking of credibility

Source: Survey Data

Table 4-7: Ranking of benevolence

Benevolence		Frequency	Percent
Valid	1st choice	107	48.6
	2nd choice	64	29.1
	3rd choice	38	17.3
	4th choice	11	5.0
	Total	220	100.0

Source: Survey Data

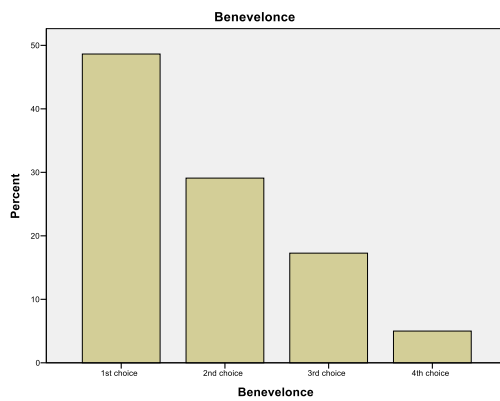


Figure 4.4: Ranking of benevolence

Source: Survey Data

Table 4-8: Ranking of Structural Assurances

Structural Assurance		Frequency	Percent
Valid	1st choice	36	16.4
	2nd choice	30	13.6
	3rd choice	84	38.2
	4th choice	70	31.8
	Total	220	100.0

Source: Survey Data

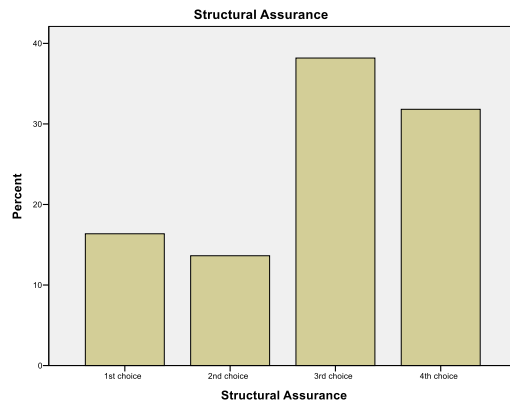


Figure 4.5: Ranking of Structural Assurances

Source: Survey Data

Table 4-9: Ranking of Firm Reputation

Firm reputation		Frequency	Percent
Valid	1st choice	21	9.5
	2nd choice	9	4.1
	3rd choice	54	24.5
	4th choice	136	61.8
	Total	220	100.0

Source: Survey Data

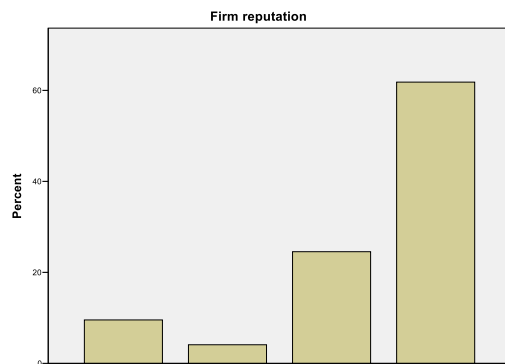


Figure 4-6: Ranking of Firm Reputation

Source: Survey Data

According to the above mentioned tables and graphs, it is quite evident that benevolence is the most preferred trust elements of the mobile banking applications users. 48.6% of respondents have ranked benevalence as No.1.

53.6% respondents have marked credibility as No.02 making it the second most anticipated trust element. 38.2% of the respondents have ranked structual assurances as No.03 ranked trust element and 61.8% of the respondents have ranked firm reputation as the No.4 ranked trust element.

Most Importnt Security Feture for Current Users of Mobile Banking Applications

Table 4-10: Most Important Security Feature

Sappusecontin Frequencies				
		Responses		Percent of Cases
		N	Percent	
Sappusecontin ^a	Access control	209	42.0%	95.0%
	Ability to perform	201	40.4%	91.4%
	Real time e-mail	49	9.8%	22.3%
	Time to time security upgrade	39	7.8%	17.7%
Total		498	100.0%	226.4%

a. Dichotomy group tabulated at value 1.

Source: Survey Data

According to table 4.10, access control is the most important security feature for the current users of mobile banking applications. It's percentage is 95%. Ability to perform transactions through the app safely is the second important security feature of the current mobile banking applications marking its percentage as 91.4%. Real time e mail and SMS alerts is the next important security aspect for the customers and its percentage is 22.3%. The least important security feature in the current mobile banking applications according to the users is time to time security upgrades done by the bank and its percentage is 17.7%.

Most Important Anticipated Security Feature of Mobile Banking Applications

Table 4-11: Most Anticipated Security Feature

\$sugincresec Frequencies

	Responses		Percent of Cases
	N	Percent	
\$sugincresec ^a multyfacauth_18	204	33.6%	92.7%
addfingprin_18	204	33.6%	92.7%
warnunsecon_18	117	19.3%	53.2%
elecsign_18	41	6.8%	18.6%
warnabnsusacti_18	41	6.8%	18.6%
Total	607	100.0%	275.9%

^a. Dichotomy group tabulated at value 1.

Source: Survey Data

According to Table 4.11, multi factor authentication and addition of fingerprinting technologies to mobile banking applications have become the most anticipated security features from the view point of the customers. In other words, customers expect that banks should introduce those features to their mobile banking applications in the future. Alerts and warnings about unsecured connections has been placed in 3rd position in terms of anticipated security features marking its percentage as 19.3%. Finally, Setting up electronic signatures and real time warnings about abnormal and suspicious activities have scored equal 6.8% placing them as the least anticipated security features from the customers' point of view.

CHAPTER 5

5 Discussion, Conclusions and Recommendations

5.1 Introduction

This chapter is dedicated for the discussion about the outcomes of data analysis. In this chapter the researcher attempts to make judgments and conclusions based on the outcomes of the data analysis. Then it is expected to come to an overall conclusion about the study and ultimately to give recommendations. Further research areas on the research problem are also presented at the end of this chapter.

5.2 Discussion On Findings

5.2.1 Finding One

The first finding is based on the first research objective. The first objective of the research is to investigate the degree of security of mobile banking applications perceived by the users of mobile banking applications. According to descriptive statistics, mean value of the perceived degree of security of mobile banking applications is 3.94. The mean value is at above average level. Therefore, it can be concluded that mobile banking applications users have an above average perceived degree of security of mobile banking applications that they are using.

The standard deviation of perceived degree of security of mobile banking applications is 0.72. This comparatively higher level of dispersion shows a higher degree to which perceived degree of security of mobile banking applications tend to spread about the mean. Therefore, it can be concluded that mobile banking applications users are comparatively much variable, less stable, less uniform and less consistent in terms of perceived degree of security of mobile banking applications that they are using.

5.2.2 Finding Two

The second finding is based on the second research objective. The second objective of the research is to investigate the degree of trust of mobile banking applications users. According to descriptive statistics, mean value of user trust is 3.83. The mean value is at above average level. Therefore, it can be concluded that mobile banking applications users have an above average trust regarding the mobile banking applications that they are using.

The standard deviation of degree of trust of mobile banking applications is 0.77. This comparatively higher level of dispersion shows a higher degree to which the level of trust regarding mobile banking applications tend to spread about the mean. Therefore, it can be concluded that mobile banking applications users are comparatively much variable, less stable, less uniform and less consistent in terms of trust they have regarding the mobile banking applications that they are using.

5.2.3 Finding Three

The third finding of the research is based on the third objective of the research which is to investigate whether the perception of the users of mobile banking applications regarding the degree of security of mobile banking applications significantly related to user trust. In order to come to a conclusion on this, the first hypothesis was formulated. According to the first hypothesis, related null hypothesis is, there is no relationship between perceived degree of security of the mobile banking applications and user trust and the relevant alternative hypothesis is, there is a relationship between perceived degree of security of mobile banking applications and user trust. In order to test the hypothesis, Pearson Product Correlation Coefficient was deployed. According to the statistical analysis, Pearson Correlation Coefficient is 0.854 which is positive. Therefore, statistical evidence is there to accept the alternative hypothesis. This indicates that there is a strong positive correlation between perceived degree of security of the mobile banking applications and user trust. This is supported by the findings of the research carried out by Kaya (2013) which recognize one factor as a strong reason for the users of mobile banking applications not to adopt mobile banking and it is their concerns for security. The same author highlighted that one of the main reasons for lower adoption for mobile banking and use of mobile banking applications is the concerns of security. Apart from that in their research findings Kim et

al (2009) point out that relative benefits, propensity to trust and security assurances had a significant effect on initial trust of mobile banking.

Therefore, it is quite evident that there are both literature and statistical evidence to claim that there is a strong relationship between the users' perceived degree of security of mobile banking applications and the trust they have over the mobile banking applications that they are using for their banking transactions. Therefore, if the banks provide more and trustworthy security to the transactions done through the mobile banking applications that their customers are using, banks can gain more trust of their customers regarding the mobile banking applications that they have introduced to the customers. Through this the banks have a very productive opportunities to enhance the use of their mobile banking applications and improve profitability by reducing cost.

5.2.4 Finding Four

Finding four is based on the fourth research objective and it is to investigate the most important trust element from the customers' point of view. In the questionnaire, respondents were asked to rank the most important trust element for them by providing four trust elements and their descriptions. According to the respondents, following are the rankings given for the trust elements.

According to this finding, the most sought trust element is benevolence. According to Lee & Chung (2009) benevolence is the belief that business partners have the necessary motivation and intent to provide benefits. Therefore, if the banks take steps to position in their customers that they have the necessary motivation to provide security for mobile banking applications, they can gain more and more customer trust. The second most sought trust element of the mobile banking applications is credibility. According to the above-mentioned authors credibility is the belief that business partners would fulfill their roles reliably and effectively. Therefore, if the management of the banks work efficiently and effectively to provide adequate security to mobile banking applications and communicate the same to the customers, banks can gain more customer trust.

5.2.5 Finding Five

Finding five is based on the fifth research objective and it is to investigate the most important security feature for the users which are available in current mobile banking applications. In this research, the respondents were requested to select the security features that are most important to them according to their perception. According to data analysis, the most preferred security features of the customers who are currently using mobile banking applications is access control. Therefore, it is quite clear that mobile applications need to have a strong access control mechanism to gain customer trust. Having a strong access control system is very important to retain the existing loyal customers as well.

The second most sought security feature by the existing banking customers is the ability to perform banking transactions through the app safely. To enable the users to perform their banking transactions safely through the banking applications, banks need to go for efficient and effective security controls with the application platform and upgrade them continuously. Through that bank will be able to gain more and more customer trust.

5.2.6 Finding Six

Finding six is based on the sixth research objective and it is to investigate the security features which can be added to enhance security of mobile banking applications. In the research, the respondents were asked to select the security features which the respondents think should be developed in the mobile banking applications they are using. According to data analysis, majority of the respondents think that using multi factor authentication can ensure much security in mobile banking applications. Here the respondents are in the view that granting access to the mobile banking application providing only one piece of evidence is not enough. Rather applications should be developed in such a way that two or more evidence presenting is needed to grant access to mobile banking applications.

The second most anticipated development in mobile banking applications is introduction of fingerprinting facilities to the applications. Customers think that adding fingerprinting facilities to mobile banking applications will enhance security of mobile banking applications rather than old fashioned user names and passwords.

5.3 Conclusion and Recommendations

Findings of this research confirm the arguments made by researchers regarding the relationship that exists between security of mobile banking applications and user trust. Statistical analysis indicated a strong positive correlation between security of mobile banking applications and user trust. When mobile applications security is high, trust on those mobile applications in the minds of the customers also high. If security of mobile banking applications is at a lower level, customer trust about the mobile banking applications would also remain at lower level. The implication of the finding is that, if bankers can establish and maintain quality security levels for the mobile banking applications that they have introduced to their customers, it is possible to gain more trust from the existing customers and potential customers. This will in the long run result in reduction of cost of service and increased productivity and profitability of the banks.

The fact that there is a strong positive correlation between security of mobile banking applications and user trust is also supported by the relevant literature that this researcher highlighted in previous chapters. Therefore, through this research it becomes very obvious that banks should improve security of the mobile banking applications that they have introduced to their customers in order to attract more and more customers to use their mobile banking applications and retain the existing customers. If proper security is not there, customers tend to refrain from using mobile banking applications and instead they would prefer traditional way of physically going to banks, stay in counters and perform their needed banking transactions. This research is done in Sri Lankan context and this research reveals that security is one of the very important and main considerations for customers to adopt to mobile banking applications rather than traditional banking approach. Through this research outcome banks can identify how important security of mobile transactions for customers and take every possible action to ensure banking applications security and communicate the same to customers.

Since there is a strong positive correlation between level of security of mobile banking applications perceived by the users and user trust, it is very important for the banks to take necessary steps to improve security of mobile banking applications. At the same time, banks should communicate effectively to the customers that their applications are secure.

Then more and more customers can be attracted to the bank. It is advisable to the banks to invest in technological advancements in the field of mobile banking application paying much attention to improve security.

Now the questions arises as to how to enhance security of mobile banking applications, what are the possible ways and means to establish a sound security for mobile banking applications. The answer lies in the research itself. In this research, the researcher identified that authentication, security controls and protection from external attacks are the key elements of mobile banking applications security. Therefore, in order to enhance security to gain more customer trust, banks and application developers should focus on those security elements. Here, authentication should be much strengthened, security controls like limits of incorrect logins and automatic time out should be introduced and strengthen in applications and sound protection from external threats such as hackers, viral attacks and social engineering attacks should be ensured.

Through this research it is now very obvious that there is a strong positive relationship between security of mobile banking applications and user trust. As a result, it is prudent to pay the attention to enhancing security of mobile banking applications to gain more customer trust. When formulating strategies to enhance security, it is important to identify the user perception about currently existing security features of currently available mobile banking applications and also to find out what are those features customers mostly want. As an answer for that, the research revealed that access control systems and ability to perform transactions through the application are the most important existing security control measures for the customers. In other words, when it comes to security features deployed for currently used mobile banking applications, customers most preferred security features are access control and transactions safety. Therefore, it is very important for banks to improve these two aspects in order to retain current loyal customers. If the customers feel that these two aspects are getting weaker in the mobile banking applications used by them, there is a risk that they will stop using mobile banking applications or move towards a competitor. Therefore, it can be recommended for the banks to improve access control and security controls in the application platform to gain trust of the users.

Since there is a strong positive relationship between security of mobile banking applications and user trust, it is very important for banks and applications developers to identify security features that can be added to mobile banking applications in order to enhance security. This research has provided the opportunity for the developers and banks to identify them through the users itself. According to the research findings, most anticipated mobile banking applications security measures which customers think that should be in mobile banking applications are multi factor authentication and fingerprinting facilities. Customers are in the view that banks should include these features to enhance security of mobile banking applications. Therefore, it can be recommended for banks to develop the mobile banking applications with multi factor authentication and fingerprinting facilities. Most of today's banks deploy password or PIN method for user authentication. Rather than stopping from one aspect, banks can move to develop their mobile banking applications in such a way that two or more pieces of information about the user are needed to give access to the application. In today's context a lot of mobile applications are equipped with fingerprinting technology. Banks can introduce it to their mobile applications as well to ensure security. Through that, banks will be able to gain trust from the existing customers and potential customers.

The ultimate outcome of this research is that there is a strong positive relationship between security of mobile banking applications and user trust. Whilst ensuring sound security for mobile banking applications, it would be beneficial for banks to identify the most valued trust aspect from the point of view of the customers in order to formulate strategies to promote mobile banking applications among customers. Although banks and developers establish a sound security background for mobile banking applications, those become useless if customers are not properly communicated about the security measures taken and if banks do not show the intent to attend to security needs of the customers. When banks identify the most sought trust aspect of the customers, it becomes easy for the banks to convey the customers about how secure their mobile banking applications are and thus attract much customer trust. Therefore, this research has helped to identify the most sought trust aspect by customers and accordingly the most sought trust element by the customers is benevolence. According to literature, benevolence is the perception of the customers that one party has the necessary motivation to provide benefits to the other party. Therefore, in

order to attract people who are not using mobile banking applications to use mobile banking applications, banks should always pay attention to the security related needs of the customers and fulfil them by time-to-time upgrading security of mobile banking applications. Banks also can-do time to time market surveys to ascertain the customer security needs when it comes to mobile banking.

5.4 Limitations of the research

This research measured the perception of the customers regarding the mobile banking applications security. Therefore, there is a limitation that perception errors cannot be mitigated in the responses of the users. Apart from that, this research does not cover the bankers' side regarding the security of mobile banking applications. Finally, this research was conducted based on a sample of individuals who are currently using mobile banking applications. Therefore, perceptions of the individuals who are not using mobile banking applications regarding the security of mobile banking applications does not cove in this study.

5.5 Further research area

Further research can be done about the technical aspects that can be used to enhance the security of mobile banking applications. Apart from that, research can be carried out with respect to the individuals who are not currently using mobile banking applications to ascertain their requirements and take actions to fulfil those to attract them to use mobile banking applications.

References

- Akturan, U., & Tezcan, N. (2011). Mobile banking adoption of the youth market: Perceptions and intentions. *Marketing Intelligence and Planning*.
- Alafeef, M., Singh, D., & Ahmad, K. (2011). Influence of Demographic Factors on the Adoption Level of Mobile Banking Applications in Jordan. *Research Journal of Applied Sciences*.
- Anyasi, F., & Otubu, P. (2009). Mobile Phone Technology in Banking System: Its Economic Effect. *Research Journal of Information Technology*.
- Barnes, S., & Corbit, B. (2003). Mobile Banking: Concept and Potential. *International Journal of Mobile Communications*.
- Bojjagani, S., & Sastry, V. (2016). Security Testing for Android Mobile Banking Apps. *Springer International Publishing*.
- Bucko, J. (2016). Security of Smart Banking Applications in Slovakia. *Journal of Theoretical and Applied Electronic Commerce Research*.
- Chandran, R. (2014). *Pros and cons of mobile banking*.
- Chen, S., Su, T., Fan, L., Meng, G., Xue, M., Liu, Y., & Xu, L. (2018). Are Mobile Banking Apps Secure? What Can Be Improved? *Jint European Software Engineering Conference and Symposium*.
- Elkhodr, M., Shahrestani, S., & Kourouche, K. (2012). A proposal to Improve the Security of Mobile Banking Applications. *International Conference on ICT and Knowledge Sharing*.
- Emmanuel, M., Hashim, L., & Adamu, R. (2016). Observed Demographic Differentials in User Perceived Satisfaction on the Usability of Mobile Banking Applications. *Knowledge Management International Conference 2016*.
- Harrison, R., Flood, D., & Duce, D. (2013). Usability of Mobile Applications: Literature review and rationale for a new usability model. *Journal of Interaction Sciences*.
- Henry Muccini, F. A. (2010). Software Testing of Mobile Applications: Challenges and Future Research Directions.

- Jabri, I. A., & Sohail, M. (2012). Mobile Banking Adoption: Application of Diffusion of Innovation Theory. *Journal of Electronic Commerce Research*.
- Johnson, S., Twilley, N., Zhang, T., Zhou, Z., & Wu, S. (2012). *Mobile Computing: A look at concepts, problems and solutions*.
- Kaya, M. (2013). *Trust and Security Risks in Mobile Banking*. Oxford.
- Kim, G., Shin, B., & Lee, H. (2009). Understanding dynamics between initial trust and usage intentions of mobile banking. *Info Systems Journal*.
- Lee, H., Zhang, Y., & Chen, K. (2013). An Investigation of Features and Security in Mobile Banking Strategy. *Journal of International Technology and Information Management*.
- Lee, K., & Chung, N. (2009). Understanding factors affecting trust in and satisfaction with mobile banking in Korea: A modified DeLone and Mc Lean's model perspective. *Interacting with computers*.
- Manali, M. (2014). *Strategic Benefits and Challenges of Mobile Banking in Kenyan Commercial Banks*.
- Nyamtiga, B., Sam, A., & Laizer, L. (2013). Enhanced Security Model for Mobile Banking Systems in Tanzania. *International Journal of Technology Enhancements and Emerging Engineering Research*.
- Pandey, P. (2019). *Mobile Banking: History and what it does*.
- Pousttchi, K., & Schurig, M. (2013). Assessment of Today's Mobile Banking Applications from the View of Customer Requirements. *Hawai International Conference on System Sciences*.
- Sun, B., Sun, C., Liu, C., & Gui, C. (2017). Research on Initial Trust model of Mobile Banking Users. *Journal of Risk Analysis and Crisis Response*.

- Akturan, U., & Tezcan, N. (2011). Mobile banking adoption of the youth market: Perceptions and intentions. *Marketing Intelligence and Planning*.
- Alafeef, M., Singh, D., & Ahmad, K. (2011). Influence of Demographic Factors on the Adoption Level of Mobile Banking Applications in Jordan. *Research Journal of Applied Sciences*.
- Anyasi, F., & Otubu, P. (2009). Mobile Phone Technology in Banking System: Its Economic Effect. *Research Journal of Information Technology*.
- Barnes, S., & Corbit, B. (2003). Mobile Banking: Concept and Potential. *International Journal of Mobile Communications*.
- Bojjagani, S., & Sastry, V. (2016). Security Testing for Android Mobile Banking Apps. *Springer International Publishing*.
- Bucko, J. (2016). Security of Smart Banking Applications in Slovakia. *Journal of Theoretical and Applied Electronic Commerce Research*.
- Chandran, R. (2014). *Pros and cons of mobile banking*.
- Chen, S., Su, T., Fan, L., Meng, G., Xue, M., Liu, Y., & Xu, L. (2018). Are Mobile Banking Apps Secure? What Can Be Improved? *Jint European Software Engineering Conference and Symposium*.
- Elkhodr, M., Shahrestani, S., & Kourouche, K. (2012). A proposal to Improve the Security of Mobile Banking Applications. *International Conference on ICT and Knowledge Sharing*.
- Emmanuel, M., Hashim, L., & Adamu, R. (2016). Observed Demographic Differentials in User Perceived Satisfaction on the Usability of Mobile Banking Applications. *Knowledge Management International Conference 2016*.
- Harrison, R., Flood, D., & Duce, D. (2013). Usability of Mobile Applications: Literature review and rationale for a new usability model. *Journal of Interaction Sciences*.
- Henry Muccini, F. A. (2010). Software Testing of Mobile Applications: Challenges and Future Research Directions.

- Jabri, I. A., & Sohail, M. (2012). Mobile Banking Adoption: Application of Diffusion of Innovation Theory. *Journal of Electronic Commerce Research*.
- Johnson, S., Twilley, N., Zhang, T., Zhou, Z., & Wu, S. (2012). *Mobile Computing: A look at concepts, problems and solutions*.
- Kaya, M. (2013). *Trust and Security Risks in Mobile Banking*. Oxford.
- Kim, G., Shin, B., & Lee, H. (2009). Understanding dynamics between initial trust and usage intentions of mobile banking. *Info Systems Journal*.
- Lee, H., Zhang, Y., & Chen, K. (2013). An Investigation of Features and Security in Mobile Banking Strategy. *Journal of International Technology and Information Management*.
- Lee, K., & Chung, N. (2009). Understanding factors affecting trust in and satisfaction with mobile banking in Korea: A modified DeLone and Mc Lean's model perspective. *Interacting with computers*.
- Manali, M. (2014). *Strategic Benefits and Challenges of Mobile Banking in Kenyan Commercial Banks*.
- Nyamtiga, B., Sam, A., & Laizer, L. (2013). Enhanced Security Model for Mobile Banking Systems in Tanzania. *International Journal of Technology Enhancements and Emerging Engineering Research*.
- Pandey, P. (2019). *Mobile Banking: History and what it does*.
- Pousttchi, K., & Schurig, M. (2013). Assessment of Today's Mobile Banking Applications from the View of Customer Requirements. *Hawai International Conference on System Sciences*.
- Sun, B., Sun, C., Liu, C., & Gui, C. (2017). Research on Initial Trust model of Mobile Banking Users. *Journal of Risk Analysis and Crisis Response*.