Trust & Security issues in Mobile banking and its effect on Customers

Muhammad Bilal
GaneshSankar

School of Computing
Blekinge Institute of Technology
SE – 371 79 Karlskrona
Sweden
This thesis is submitted to the School of Computing at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 2x20 weeks of full time studies.

Contact Information:
Authors(s):
Muhammad Bilal,
E-mail:mubg08@student.bth.se
Ganesh Sankar
E-mail:gshindi@gmail.com

University advisor(s):
Jenny Lundberg, PhD
School of Computing

School of Computing
Blekinge Institute of Technology
SE – 371 79 Karlskrona
Sweden

Internet : www.bth.se/com
Phone : +46 455 38 50 00
Fax : +46 455 38 50 57
**ABSTRACT**

**Context:** The invention of mobile phones makes the human life easier. The purpose of this study is to identify security risks in mobile banking and to provide an authentication method for mobile banking transaction by using bio-metric mechanism.

**Objectives:** Current mobile banking authentication is challenging and identified as a major security risk. Literature review shows that customer distrusts mobile banking due to security issues. The authors discuss security risks in current authentication methods in mobile banking.

**Methods:** There are different methods and approaches to handle authentication in mobile banking. In this thesis, we propose a new approach of authentication in mobile banking. The strengths and weaknesses of existing approaches of authentication are identified with the help of Literature Review and interviews. The authors present basic transaction model and include security risks. By Literature Review it is found that finger print mechanism is a suitable method for authentication. Authors focus on authentication method and present a biometric scanning device which can identify the customer’s finger print thus enabling the customer to access mobile banking facility.

**Results:** An authentication model is proposed through design process. The proposed biometric design was validated by conducting a workshop. The analysis of the workshop’s results showed that customer’s trust in security for mobile banking will be increased by finger print mechanism. To promote mobile banking, it is necessary to improve customer trust in terms of security.

**Conclusions:** The authors concluded that, only authorized person will be able to use mobile banking services by incorporating bio-metric finger-print mechanism. By literature review and interview it was found that finger-print mechanism is more suitable than other ordinary mechanisms like login and password mechanism, SMS etc.

**Keywords:** Trust, Security Authentication, bio-metric finger print
# CONTENTS

TRUST & SECURITY ISSUES IN MOBILE BANKING AND ITS EFFECT ON CUSTOMERS ........................................................................................................................................................................... 1

ABSTRACT ........................................................................................................................................................................... 2

CONTENTS ........................................................................................................................................................................... 3

LIST OF TABLES ................................................................................................................................................................... 6

LIST OF FIGURES ................................................................................................................................................................... 7

1 INTRODUCTION ........................................................................................................................................................... 8

1.1 PROBLEM DEFINITION ........................................................................................................................................... 9
1.2 OBJECTIVES .............................................................................................................................................................. 9
1.3 EXPECTED OUTCOME ............................................................................................................................................ 9
1.4 RESEARCH QUESTIONS ......................................................................................................................................... 9
1.5 RESEARCH METHODOLOGY ................................................................................................................................. 9
1.6 RESEARCH DESIGN .................................................................................................................................................. 10
1.7 THESIS OUTLINE ..................................................................................................................................................... 10

2 BACKGROUND ................................................................................................................................................................ 12

2.1 RELATED TERMS...................................................................................................................................................... 12

2.1.1 Trust in mobile banking .................................................................................................................................. 12
2.1.2 Trustworthy design for mobile banking ......................................................................................................... 14
2.1.3 Mobile Payment ................................................................................................................................................ 14
2.1.4 Mobile Commerce .......................................................................................................................................... 14
2.1.5 Authentication .................................................................................................................................................. 14
2.1.6 Human Computer Interaction (HCI) ............................................................................................................. 14
2.1.7 Design in Human Computer Interaction (HCI) ............................................................................................. 15

3 SECURITY ISSUES IN MOBILE BANKING ..................................................................................................................... 16

3.1 LITERATURE REVIEW .......................................................................................................................................... 16

3.1.1 Search Strategy .................................................................................................................................................. 16
3.1.2 Primary Search ................................................................................................................................................ 16
3.1.3 Secondary Strategy ........................................................................................................................................ 17
3.1.4 Search String ................................................................................................................................................... 17
3.1.5 Criteria for study selection .............................................................................................................................. 17

3.2 PROCEDURE FOR THE SELECTION OF PAPERS ................................................................................................. 17

3.2.1 Procedure for data selection .......................................................................................................................... 17
3.2.2 Information about research articles ............................................................................................................. 18
3.2.3 Relevant area of study ...................................................................................................................................... 18
3.2.4 Review Conducted ........................................................................................................................................... 18
3.2.5 Study selection ................................................................................................................................................ 18
3.2.6 Identifying Risks in current mobile banking ................................................................................................. 20
3.2.7 Proposing Biometric mechanism for mobile banking .................................................................................. 20
3.2.8 Conducting Workshop .................................................................................................................................. 20
3.2.9 Analysis phase ................................................................................................................................................ 20

3.3 MOBILE BANK TRANSACTION SERVICES MODEL .............................................................................................. 21

3.4 SECURITY ISSUES IN MOBILE BANKING .......................................................................................................... 21

3.4.1 Mobile banking and Security issues with WAP (Wireless Application Protocol) ........................................ 21
3.4.2 Authentication Risks and Issues .................................................................................................................... 22
3.4.3 Bank provides the service directly to the customer architecture ................................................................. 22
3.4.4 Banks share their facility to 3rd party service provider ................................................................................ 23
3.4.5 SMS based Mobile banking .......................................................................................................................... 24
3.4.6 SMS encryption ............................................................................................................................................... 24
3.4.7 SMS Spoofing Attack .................................................................................................................................... 24
3.4.8 Virus Attacks in mobile banking ................................................................. 25
3.4.9 Risk with Digital Signature ........................................................................ 25
3.5 BIOMETRICS AND MOBILE BANKING .................................................... 25
  3.5.1 Vision for Secure Mobile bank transaction: .............................................. 26
4 INTERVIEW PHASE ......................................................................................... 27
  4.1 THE INTERVIEWS ....................................................................................... 27
  4.2 INDUSTRIAL INTERVIEWS ......................................................................... 27
  4.3 SELECTION OF INTERVIEW SUBJECT ...................................................... 28
  4.4 INTERVIEWING .......................................................................................... 28
    4.4.1 Designing Questions for Interview ......................................................... 28
    4.4.2 Analysis of the Interviews and Literature Review .................................... 28
5 BIOMETRICS MOBILE BANKING SYSTEM ............................................... 31
  5.1 PROPOSED BIOMETRIC MECHANISM .................................................. 31
    5.1.1 Bio-Metric .............................................................................................. 31
    5.1.2 Proposed Mechanism .......................................................................... 31
    5.1.3 Bio metric Authentication method in Mobile banking Model ................. 31
    5.1.4 Proposed Bio metric Mobile Banking System diagram ........................ 32
    5.1.5 Biometric Fingerprint Scanner device ................................................ 33
  5.2 MOBILE BANKING MECHANISM THROUGH FINGER PRINT ............ 34
  5.3 LDAP (LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL) WORKING MECHANISM FOR SECURITY PURPOSES ................................................. 36
  5.4 AUTHENTICATION AND AUTHORIZATION MECHANISM .................... 37
6 WORKSHOP ..................................................................................................... 39
  6.1 AN OVERVIEW ............................................................................................ 39
  6.2 AIM AND OBJECTIVES .............................................................................. 39
  6.3 PARTICIPANTS ............................................................................................ 39
  6.4 ACTIVITIES ................................................................................................ 39
    6.4.1 Welcome and Introduction ................................................................. 39
    6.4.2 Presentation ......................................................................................... 39
    6.4.3 Discussion Session .............................................................................. 40
  6.5 QUESTIONNAIRE ...................................................................................... 41
  6.6 FEEDBACK ................................................................................................. 41
7 ANALYSIS PHASE .......................................................................................... 45
  7.1 TRUST IN MOBILE BANKING .................................................................. 45
  7.2 SECURITY ISSUES IN MOBILE BANKING ............................................. 45
  7.3 SECURE AUTHENTICATION METHOD .................................................... 45
  7.4 PROPOSED FINGER PRINT AUTHENTICATION MECHANISM ................ 46
  7.5 WORKSHOP .............................................................................................. 46
8 VALIDITY .......................................................................................................... 47
  8.1 CREDIBILITY .............................................................................................. 47
  8.2 TRANSFERABILITY ..................................................................................... 47
  8.3 DEPENDABILITY ......................................................................................... 48
  8.4 OBJECTIVITY ............................................................................................. 48
9 EPILOGUE ......................................................................................................... 49
  9.1 CONCLUSION ............................................................................................ 49
  9.2 ANSWERS TO THE RESEARCH QUESTIONS .......................................... 49
  9.3 FUTURE WORK .......................................................................................... 50
REFERENCES ...................................................................................................... 51
10 APPENDIX B ................................................................................................. 55
  10.1 INTERVIEW QUESTIONS .......................................................................... 55
    TRANSCRIBED INTERVIEWS ...................................................................... 56
11 APPENDIX B ................................................................................................. 60
LIST OF TABLES

Table 1: Research question design ................................................................. 10
Table 2: Journals, Conferences and books .................................................. 19
Table 3: Selected Articles during conducting LR ......................................... 20
Table 4: Security threads for mobile banking ............................................. 22
Table 5: Improving electronic banking Security with Bio metrics method .... 26
Table 6: Current mobile banking system ...................................................... 29
Table 7: Bio metric Mobile banking ............................................................. 30
Table 8: Key points of discussion ............................................................... 40
Table 9: Percentage of criteria of the proposed bio metric mobile banking ... 42
LIST OF FIGURES

Figure 1: Research Design ........................................................................................................ 10
Figure 2: Risks in mobile bank services for the customers ..................................................... 21
Figure 3: provides the service directly to customer architecture [40] ........................................ 23
Figure 4: Banks share their facility to 3rd party service provider ........................................... 23
Figure 5: Simple biometrics system architecture .................................................................... 26
Figure 6: The finger print method for authentication in mobile banking ................................ 31
Figure 7: Flowchart of proposed bio metric mobile banking system ....................................... 32
Figure 8: Proposed Finger Print Scanner ................................................................................ 33
Figure 9: Working Mechanism of LDAP .............................................................................. 36
Figure 10: Mechanism to connect Web server/database and LDAP Services ......................... 37
Figure 11: Customer accessing Mobile banking ...................................................................... 37
Figure 12: Percentage of Response of Questionnaire analysis .............................................. 42
Figure 13: participants strong agree factors analysis about biometric authentication method for mobile banking .......................................................... 43
Figure 14: Participants preference for finger print authentication ............................................ 43
Figure 15: Trust and Security analysis in workshop .............................................................. 44
1 INTRODUCTION

Forrester research reported that the number of people using internet through mobile phones is 219 million across the world and 1.5 billion users use mobile phones, which is three times more than the number of people using personal computers (PCs)[1][2]. In future, mobile phones could be taken as a substitute to personal computers (PCs)[3]. Using mobile phones for mobile banking, customers can push or pull the details like Funds transfer, Bill payment, Share trade, Check order and also inquiries like Account balance, Account statement, Check status Transaction history etc. It means that the customer is interacting with the files, databases etc., of the bank [4]. Database at the server end is sensitive in terms of security. Customers distrust mobile devices to transfer money or for making any transactions. The reason is that security is a major concern for the customer’s fulfillment. Customer’s main concern in using mobile devices for mobile banking is the authentication method used to ensure that the right person is accessing the services like transaction etc[5][6]. A third party payment gateway is involved in this mobile payment scheme; they give service between two or more banks so the customers need to trust on unknown third-party payment gateway and also need to pay an extra service charge [6].

If the customer loses his/her mobile phone then there is no assurance that there is safety in using current mobile banking authentication mechanism. For example, if a person stores the password in mobile phone for reference then an unknown person can easily utilize the customer’s account. Due to advancement in technology, customers and organizations take interest in Biometrics technology to reduce the uncertainty and security concern. Biometrics authentication mechanism is to identify the physical individuality or uniqueness of the authorized person [7].

Authentication can be performed by PIN number or user name and Password, ID card, etc. Finger print recognition system is a part of biometric system. The advantage of using fingerprint is that, communication can occur only through authorized persons and will be secure. Fingerprint technology is the most commonly used in telecommunication industry [8]. Security is highly concerned while making mobile payment. Presently personal information can be lost when any person loses their mobile handset [9]. If fingerprint technology is introduced in mobile phones, then the risk of unauthorized persons using the mobile for mobile banking is significantly reduced.

For mobile banking, it is necessary to have a biometric method (Fingerprint) through which customer can access the bank account and performs mobile banking activities like e-commerce etc.

By literature Review the authors identified that customers did not trust mobile banking payment transaction. Through literature review the authors identified that customer mainly distrusts the authentication and level at which data transactions are made securely.

The authors made a basic model for mobile banking transaction. All security risks were included in the transaction model. Then the authors focused on authentication method. By literature review and interview it was concluded that security can be improved by bio metric methods. The authors focused on different bio-metric mechanism and concluded that fingerprint mechanism is more suitable as it requires less storage capacity in database and identifies the uniqueness of customers. The authors suggest a possible solution by proposing finger-print mechanism model and designed a bio-metric scanning device as a solution through which customer can interact with banking system using their finger-print.
1.1 Problem Definition
Security is the main issue for mobile banking [8]. Trust can be developed through secure transition between bank and the customer’s mobile phone. Proper identification of the authorized user is lagging in current mechanism. Loss of mobile phone can result in insecurity for the mobile banking customers.

1.2 Objectives
The objective of this study is to develop a design model that implements the concepts of using biometric authentication method to reduce risks of fraud and to improve customer’s trust in mobile banking [8][9]. Finger-print takes only 256 bytes and its accuracy is high. The biometric device first captures the user’s finger print and creates a reference template and it is stored in database and that ends the enrolling processes of user’s finger print [10]. The objective also includes the following.
- Identifying reasons why customer distrust mobile banking
- Making a basic mobile banking transaction model and identifying security risks in mobile banking.
- Proposing Biometric finger-print mechanism for authentication to improve customer trust and self-satisfaction for mobile banking adoption for money transaction.

1.3 Expected Outcome
The authors propose transaction model for mobile banking. The basic model of mobile banking shows security issues and risks. The authors propose biometric model for mobile bank transaction and bio-metric (Finger Print) authentication method for mobile banking.

1.4 Research Questions
The research questions that we address in our study are formulated as follows:
Research Question1: Why does customer not trust on Current Mobile Bank Transactions?
Research Question2: What are the security issues in current mobile banking?
Research Question 3: Which kind of authentication method is more suitable for the customer using mobile banking services?
Research Question 4: How bio-metrics can play an important role for secure authentication in mobile banking?

1.5 Research Methodology
i. For Research Question 1: By LR first authors will discuss the customer distrust about current security when mobile customer is using mobile banking services.
ii. For Research Question 2: By LR [11] the security issue is illustrated. For this purpose first the authors make a basic mobile bank transaction model and then add security risks in the model. Finding the risks is one of the important issues for mobile banking transaction.
iii. For Research Question 3: LR and interview show that suitable authentication method is Bio-metric finger print. Finger-print assures that authorized person is doing mobile banking and improves security level for authentication. Authors illustrate finger-print mobile bank mechanism.
iv. For Research Question 4: Study shows that finger-print is more unique and suitable as compared to other bio-metric mechanism like voice, face recognition etc. The authors explained advantages of finger-print to increase security level and improve trust.

v. At end the authors conducted workshop. The author founded the workshop is very important. Because through workshop the authors got feedback, and self-assessment of proposed finger print authentication mechanism. The authors got many suggestions about finger print authentication methods. At the end of workshop the authors distributed questionnaire for evaluation. This is explained in detail.

<table>
<thead>
<tr>
<th>Research Questions</th>
<th>Methodology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research Question No#1</td>
<td>Literature Review</td>
</tr>
<tr>
<td>Research Question No#2</td>
<td>Literature Review</td>
</tr>
<tr>
<td>Research Question No#3</td>
<td>Literature Review/ Interviews</td>
</tr>
<tr>
<td>Research Question No#4</td>
<td>Literature Review/ Interviews</td>
</tr>
</tbody>
</table>

**Result:** Proposing a mechanism for mobile banking using bio metrics method/ conducting workshop for evaluation purposes.

Table 1: Research question design

### 1.6 Research Design

![Research Design Diagram]

**Figure 1: Research Design**

### 1.7 Thesis Outline

**Chapter 1: Introduction:**

Introduction part describes the definition and goals. The authors also describe the research questions and methodology.
Chapter 2: Background

Lays the background of mobile banking and defines the related terms which are used in the thesis.

Chapter 3: Security issues

Identify the factors why customer distrusts mobile banking. Furthermore, identifying security issues between mobile devices and mobile banking systems. Finding which approach is more suitable and secure for mobile banking transaction between customer and bank. Also the authors propose a basic model for transaction in mobile banking with security risks.

Chapter 4: Interview Phase

To find a secure authentication method for mobile banking services, the authors take help from Literature Review and conduct interviews with academic and bank experts.

Chapter 5: Proposed Biometric Mechanism

The authors propose a mobile transaction model with fingerprint mechanism. The authors show a proposed biometric model for mobile banking. Authors also show the mechanism of biometric mobile banking.

Chapter 6: Workshop

The workshop was conducted in the campus of Blekinge Tekniska Högskolain which PhDs students and master students took part. The proposed finger print authentication method for mobile banking sector was described to them and their suggestions were recorded.

Chapter 7: Analysis Phase:

In analysis phase the authors presented the overview of LR, interviews and workshop.

Chapter 8 Validation

The authors presented four types of validation. Authors explained Credibility, Transferability, Dependability and objectivity.

Chapter 9 Epilogue

This chapter contains future work, conclusion and recommendations collected from experts in bank sector, academic sectors and literature review.
2 BACKGROUND

Bank services for the execution of financial services through mobile device are called Mobile banking. Security includes:

i. Data transmission: which should be securing so that no hacker should be able to hack the data, for this purpose a secure connection is needed.

ii. Authentication: only authorized persons are allowed to access the data.

iii. Authorization: This should be simple and fast so that quick access should be available for the data [12].

Mobile device helps the customer to carry out transactions at any time and from anywhere. Through mobile phones customers can get details about account, transfer money to account etc. The customers are interacting with the databases etc. of the bank. In terms of security, the data at the customer end with mobile device is as sensitive as the database at the server end. So security is an important issue for the customer trust [4].

Now users are more interested to do their financial services through mobile. Mobile banking based on WAP (Wireless Application Protocol) and SMS (Short Message Service) is popular [13]. Customers can find out the details about their account balance and will be able to get their desired data through SMS. But still there are security problems in making transaction through SMS. The data are not secure while transmitting through SMS. The reason is that, no encryption technique can be applied for sending and receiving SMS. Through WAP (Wireless Application Protocol) different types of devices can be used to access the internet. WAP is vulnerable to hacker’s attacks due to its protocol translation and compression of contents which is insecure.

From the customer point of view it is necessary to develop trustworthy systems which ensure security, privacy, data integrity and a secure full authentication between customer’s mobile phone and bank’s system for mobile banking [14].

Identifying authentication is also a vital part of security. Authentication means allowing only the authorized persons to use the mobile banking services. Authentication is very important because it is the area which ensures end-to-end security between the users mobile and bank system.

It is realized that trust in mobile banking can be developed through factors such as secure transaction, behavior of customer towards adoption of mobile banking in terms of customer and bank staff relationship [15].

In this thesis, the authors will present a framework which will overcome the current security issues between the customers’s mobile and the bank system while using the mobile banking services. Authors studied various approaches and conducting interviews in local banks to find, how to overcome security issues when the customers are using mobile banking services. By studying LR, we found out that implementing biometrics methods will minimize the security risks and thus the authors present a biometrics mechanism in which customer can use mobile banking services securely.

2.1 Related Terms

2.1.1 Trust in mobile banking

Mobile banking provides services like taking loans, retail sales or transaction of money from one account to another account [10].

Customers can receive information about their account balance through mobile devices via SMS. Due to WAP and GPRS the customer can access a wide range of services like transferring money from one account to another account, trading in stock and making payments through mobile device for purchasing items. In Europe, mobile banking gains
more popularity whereas in United State of America some of the banks have stopped their mobile banking services due to lack of trust among the customers. Security and convenience are the key factors for the growth of mobile banking and mobile commerce [16]. In mobile banking, trust is considered to be the most important factor. The reason is that the transaction of money is occurring online. Face to face contact is not possible in mobile banking. Trustworthiness is the belief that the business partner can be trusted and will act according to the business rules. Acceptance of technology and willingness of transacting money depends upon the customer trust. Customers lack trust on mobile banking because of some issues in its process like cost, security, convenience of customer in adopting mobile banking etc.

i. Convenience is an important factor because customer will take initiative to use mobile services for transferring money, purchasing products, etc only when it is easy and simple.

ii. From the customers point of view a security issue includes authorization, authentication, integrity, confidentiality and also subjective security [17].

iii. Usage cost includes cost for mobile banking services and cost for technical infrastructure like purchasing a new phone.

iv. Mobile banking trust can be developed among the customers, when less technological failure with strong form of social interaction occurs. User controlled transaction and ensuring that authorized person is using mobile device for transaction, is the important factors for Trust [18].

v. Fraudulent usage occurs because of unauthorized transactions which decreases the level of trust among mobile banking customers.

vi. The communication between mobile device and bank system must be reliable and should not fail during any transaction; making reliability an important factor in mobile banking [19].

vii. Technical failure also results in lack of customer trust on mobile banking. A new wireless technology which has RFID tag called NFC (Near Field Communication) is adopted by banks especially in Sweden. The NFC tag stores personal information and could act as car key, tickets, money etc. Up to 40% of mobile market in Europe uses NFC technology. But this technology involves risk like non-repudiation [20], Security related problems like modification and eavesdropping of data occurs in NFC technology. Suitable protocol against Man-In-The-Middle (MITM) attack is also needed in NFC [21].

viii. As electronic commerce increase in popularity among the customer day by day, it is important to prevent hacker attacks. Security failure also reduces customer trust in mobile banking system [22].

ix. More attention has been given to secure authentication method for various devices. Commonly there are two types of attacks namely MITM (Man in the middle) and malicious software (MSW). These two attacks are generally used on web browsers. Through MSW the attacker can make changes in data transacted which are submitted through web browser [23].

x. According to Bank of Korea (2008), 96% of customers using mobile banking are unsatisfied. Customers did not trust the security in wireless transaction and the transaction speed was slower [24].

xi. Developed Information System model in which they found that users trust in mobile payment transaction is very important. Because there is no face to face contact occurring in mobile banking services. According to them, system quality and information quality are the important factors for developing customer satisfaction and trust on mobile bank services [25].
2.1.2 Trustworthy design for mobile banking

The manufacturers of mobile phones have to design the mobile device in such way that mobile phones can prevent unauthorized access by attackers thus maintaining privacy and safety for money transactions. To achieve customer’s trust, the manufacturers must concentrate on the security issues related to mobile banking. Authentication in mobile banking is one of the core issues [26].

2.1.3 Mobile Payment

Using mobile device for their payment is called mobile payment. Through mobile payment you can do such as buying items, booking tickets etc. so we can say that mobile payment is the relationship between customers, business, and bank domain [6]. Nowadays mobile payment needs more research work because mobile payment will empower the commerce field an advantage for the banks in term of revenue. A secure and trusted transaction will create more interest for the adopting of mobile payment. The advantage of mobile payment is that customer will not pay via cash or credit card [27].

2.1.4 Mobile Commerce

Mobile commerce is using mobile devices for commercial services like buying, selling, exchange of goods between customers and financial institutions [28]. Mobile devices are user friendly and it is an easy way for buying products. Mobile phones are small portable devices through which customers cannot only access the information all over the world but also perform business transactions which are the reasons why mobile commerce is gaining more attention from the users [29]. The technical requirement in mobile commerce is a satisfactory transmission network of payment systems between sellers and buyers [30]. The important area of mobile commerce is the security in mobile payment and network technology. Making commercial transactions through mobile phone requires high level of security [31].

2.1.5 Authentication

Authentication is a process through which we identify that a particular device is allowed to use an application. Authentication is the important factor for the trustful and secure use of mobile devices for accessing mobile banking services. Nowadays security and privacy are especially important for mobile device. Authentication means that only authorized persons are allowed to use mobile phone for their daily services. There are different types of authentication methods, for example user name and password method, bio metrics methods etc [32].

It is noted that by using biometric method, fraud can be minimized. To prevent the attackers from hacking data and to prevent use of applications like mobile bank application etc., by unauthorized persons and to increase security, it is necessary to adopt biometrics technology for mobile banking applications. Having a more secure authentication method will result in more users adopting mobile banking services and will not hesitate to make money transaction.

2.1.6 Human Computer Interaction (HCI)

HCI is the bridge between humans and the study of technology. A wide research is ongoing in many fields related to HCI such as ergonomics, humans, information system, computer engineering, industrial engineering etc. Commonly HCI is considered as one of the main
cores of sciences and especially of computer science. The main goal of HCI is to make user friendly and easy understandable interaction environments between users and computers [33].

2.1.7 Design in Human Computer Interaction (HCI)

Design is a set of policies which helps the designers to take decisions. Through design principles, the decision makers are able to apply it in the real world. Designing is one of the main area of human computer interaction. Designing mainly focuses on the formation of information in a graphical way on how it works in reality [34].
3 Security Issues in Mobile Banking

In this chapter, the authors present a Literature Review (LR) and interviews of bank management to identify the main issues in secure transaction for mobile banking. Literature study shows that bio metric methods can improve security. On the basis of literature review and interviews with bank staff and IT experts, security issues were identified. The authors are able to present a secure mechanism using bio metrics method to perform mobile banking.

3.1 Literature Review

Literature Review [11] is one of the important phases in research work as it plays a vital role in research process. The literature review helps to define the research gap. Then research is needed for solving the problem. Basically the main aim of literature review is to identify the current issues? We choose literature review to identify the causes that customer do not trust current mobile banking. By literature review it is identified that security is the major issue in current mobile banking. To explore this we adopt a systematic approach to search available literature related to trust, Security issues in current mobile banking and its effect on customers. For this purpose the authors make a model see (Figure 2) and add all security risks when customer using mobile bank services. By literature review the authors also found that security risks can be minimized by biometric mechanism. The authors also propose a biometrics mechanism model see (Figure 6) to minimize the security risks in current mobile banking. To explore this authors adopt a systematic approach to search available literature on trust, security issues in mobile banking and its effect on customers. Additionally the semi-structured interviews were conducted. Interviews were accomplished and authors got beneficial information to support research process.

3.1.1 Search Strategy

Finding relevant papers from particular resources or databases is called Search Strategy. There are two main searching strategies for conducting the literature review, which are

i. Primary Search
ii. Secondary Search

3.1.2 Primary Search

The primary search is about searching the data relevant to the research gap/ research questions. It includes journals, online databases etc. The sources for the primary search phase are given below:

i. IEEE explore
ii. ACM Digital Library
iii. Science Direct
iv. Citeseer library (citeseer.ist.psu.edu)
v. Google scholar (scholar.google.com)
vi. Spring Link

In this thesis we mainly focused on the following databases for review:

i. IEEE explore
ii. ACM Digital Library
iii. Science Direct
iv. Google scholar (scholar.google.com)

3.1.3 Secondary Strategy

The secondary phase is associated with:
   i. Identifying the research area
   ii. Material collected in primary study
   iii. Extraction of relevant data
   iv. Monitoring of data
   v. Data synthesis

3.1.4 Search String

The aim of the thesis is
   i. To find out the relevant work by performing LR.
   ii. To find papers relevant to perform secure transaction through mobile banking services by the customer.
   iii. To develop the trust of the customer and to make them adopt mobile banking. It is necessary to find out the area of research where security is lacking.

We found some research material by using the following string:

((("Mobile banking")OR ("Mobile commerce") AND ("Security") AND ("Trust")) AND ((mobile financial service) OR (technology acceptance model) OR (structural equation model) OR (PKI) OR (Digital Certificate) OR (mobile commerce) OR (WAP) OR (e-commerce) OR (biometric security) OR (template protection) OR (Customer satisfaction) OR (Quality) OR (Fuzzy Vault) OR (finger print) OR (SMS) OR (Authentication)))

3.1.5 Criteria for study selection

The selection depends on the following criteria:
The authors selected the research papers which were from January 2000 to May 2011.
The important segment of LR is to include the important research papers.
The authors selected most important articles and research papers based on
   i. The current Trust and security issues in mobile banking.
   ii. The authentication methods for mobile banking transaction and customer satisfaction for mobile banking services.
   iii. The bio metrics methods and finding the appropriate biometric method suitable for authentication in trust and security point of view.

3.2 Procedure for the selection of papers

Authors selected articles and papers, which are related to mobile banking and authentication methods. For this purpose, articles are included in document on the basis of reading abstract.

3.2.1 Procedure for data selection

Selecting data relevant to research work from research articles.
3.2.2  Information about research articles

i. Title of the article
ii. Subtitle of the article
iii. Name of authors
iv. Information about Publication
v. Database used for searching data
vi. The year and date when the article was published

3.2.3  Relevant area of study

i. Mobile banking
ii. Customer Trust in mobile banking
iii. Current security issues in Authentication methods for mobile banking services
iv. Improving security by bio metrics method.

3.2.4  Review Conducted

The steps of LR are given below:
The research question and the information relevant to research questions were kept in mind [11].
The authors mostly found out information which includes:
- Trust and current security issues in mobile banking services?
- Discussed different mechanisms in current mobile transactions and security threads in payment transactions.

3.2.5  Study selection

Mainly the authors did study in the following steps which are given below:

i. Selection of articles
ii. Including or excluding the articles in the research study
iii. Additionally manual search was also performed using Google and Google scholar.

Articles were selected based on title name, abstract and conclusion to decide whether or not it is relevant to the research. The table below shows the selected articles.

<table>
<thead>
<tr>
<th>Journals</th>
</tr>
</thead>
<tbody>
<tr>
<td>What can you learn about cell phone</td>
</tr>
<tr>
<td>Trust in Mobile banking</td>
</tr>
<tr>
<td>Cell phone banking and security</td>
</tr>
<tr>
<td>Customer Trust in mobile banking</td>
</tr>
<tr>
<td>Trust and Security issues in mobile banking</td>
</tr>
<tr>
<td>Modeling user Trust and Mobile banking</td>
</tr>
<tr>
<td>Mobile banking Architecture</td>
</tr>
<tr>
<td>Virus effecting customer accounts</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Conferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ninth Global Mobility Roundtable (ICMB-GMR), 2010 Ninth International Conference</td>
</tr>
</tbody>
</table>
Selected articles: A total number of 93 articles were scanned in this LR and 34 were selected.

<table>
<thead>
<tr>
<th>No</th>
<th>Selected Research Articles</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Assessment of Today’s Mobile Banking Applications from the View of Customer Requirements</td>
</tr>
<tr>
<td>2</td>
<td>Customer’s Adoption Decision Analysis of Mobile Banking Service</td>
</tr>
<tr>
<td>3</td>
<td>Performance Evaluation on End-to-End Security Architecture for Mobile Banking System</td>
</tr>
<tr>
<td>4</td>
<td>Design and Evaluation of M-Commerce Applications</td>
</tr>
<tr>
<td>5</td>
<td>M-Commerce Development and Challenges Facing</td>
</tr>
<tr>
<td>6</td>
<td>M-Payment between Banks Using SMS</td>
</tr>
<tr>
<td>7</td>
<td>Mobile Payment: A Journey through existing procedures and initiatives</td>
</tr>
<tr>
<td>8</td>
<td>Using System Dynamics to Simulate the Strategic Planning of the Mobile Commerce Terminal (MCT) Industry and Mobile Commerce Diffusion</td>
</tr>
<tr>
<td>9</td>
<td>A Framework for Personal Mobile Commerce Pattern Mining and Prediction</td>
</tr>
<tr>
<td>10</td>
<td>A study on service quality assurance in mobile commerce</td>
</tr>
<tr>
<td>11</td>
<td>User Assigned Security Policy Framework for M-Commerce Applications</td>
</tr>
<tr>
<td>12</td>
<td>IPAS: Implicit Password Authentication System</td>
</tr>
<tr>
<td>13</td>
<td>Mobile Banking Information Security and Protection Methods</td>
</tr>
<tr>
<td>14</td>
<td>Research on Security Payment Technology Based on Mobile E-commerce</td>
</tr>
<tr>
<td>15</td>
<td>Critical factors of WAP services adoption: an empirical study</td>
</tr>
<tr>
<td>16</td>
<td>Four-Scenario Analysis for Mobile Banking Development Contextualized to Taiwan</td>
</tr>
<tr>
<td>17</td>
<td>Public key infrastructure for mobile banking security</td>
</tr>
<tr>
<td>18</td>
<td>Social Impact of SMS in Sri Lanka</td>
</tr>
<tr>
<td>19</td>
<td>Improving E-Banking Security with Biometrics</td>
</tr>
<tr>
<td>20</td>
<td>Cell phone banking: predictors of adoption in South Africa— an exploratory study</td>
</tr>
<tr>
<td>21</td>
<td>Four-scenario analysis for mobile banking development contextualized to Taiwan</td>
</tr>
<tr>
<td>22</td>
<td>Making secure TCP connections resistant to server failures</td>
</tr>
<tr>
<td>23</td>
<td>Business aspects of trusted third party services in Europe</td>
</tr>
<tr>
<td>24</td>
<td>A Loss Reportable E-Cash Scheme without TTP Based on ECC</td>
</tr>
<tr>
<td>25</td>
<td>Social Impact of SMS in Sri Lanka</td>
</tr>
<tr>
<td>26</td>
<td>Improving E-Banking Security with Biometrics: Modeling User Attitudes and Acceptance</td>
</tr>
<tr>
<td>27</td>
<td>Usability evaluation of multi-modal biometric verification systems</td>
</tr>
</tbody>
</table>
Table 3: Selected Articles during conducting LR

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td>Biometric recognition in telecom environment</td>
</tr>
<tr>
<td>29</td>
<td>Biometric Authentication for a Mobile Personal Device</td>
</tr>
<tr>
<td>30</td>
<td>Design of Embedded Multimodal Biometric Systems</td>
</tr>
<tr>
<td>31</td>
<td>Biometric template data protection in mobile device environment using XML-database</td>
</tr>
<tr>
<td>32</td>
<td>Biometric Mobile Template Protection: A Composite Feature Based Fingerprint Fuzzy Vault</td>
</tr>
<tr>
<td>33</td>
<td>Modeling User Trust and Mobile Payment Adoption</td>
</tr>
<tr>
<td>34</td>
<td>Understanding factors affecting trust in and satisfaction with mobile banking in Korea</td>
</tr>
</tbody>
</table>

3.2.6 Identifying Risks in current mobile banking

By studding the above articles the authors identifies security risks and add in the model. Figure 2: “Risks in mobile bank services for the customers”. This is explained in (section 3.3). Then authors explained all security issues when customer doing mobile banking services through mobile handset in (section 3.4). Supporting of identifying security risks in current mobile banking the authors also conducted semi-structured interviews which is described in chapter 4 Interview Phase.

3.2.7 Proposing Biometric mechanism for mobile banking

By LR the authors founded that security can be improved by biometric mechanism. Furthermore the authors determined that finger print is more secure and suitable method for secure authentication purposes. Through LR and interviews the authors proposed Bio metric Authentication method in Mobile banking Model in (section 5.1.3) and biometric bank mechanism which is described in chapter 5.

3.2.8 Conducting Workshop

At the end the authors conducted workshop at (Blekinge Tekniska Högskola) campus. 16 potential future users attended the workshop. The participant’s gives their positive suggestion and most of the participants agree that by minimizing security risks the customer trust will be developed to adopt mobile banking services. At the end of workshop the authors distributed questionnaire and take positive response from the participants. Which are described in chapter 6 Workshop.

3.2.9 Analysis phase

At the end authors did analysis see chapter 7. In analysis phase the authors summarizes the security factors which effects customer trust regarding mobile banking.
3.3 Mobile bank transaction services Model

Figure 2: Risks in mobile bank services for the customers

3.4 Security issues in mobile banking

Mobile banking has two zones, one is the handset held by the user and the other is the bank zone. Literature shows that possibility of security threat exists for transaction of payment using mobile device [35].

3.4.1 Mobile banking and Security issues with WAP (Wireless Application Protocol)

WAP is used for communication between devices like digital mobile phones, internet, PDA etc. Through WAP customer can realize more functionality of internet banking. Encryption process is currently used for secure data transmission between bank and users but the problem is that this encryption process is not good enough for the protection of sensitive data between bank and customer. The reason is that security methods require more powerful computing and high storage capacity. If we take internet banking it is realized that there are powerful computer systems and well defined complex encryption process to ensure the security. Mobile device have low computational capacity and hence we are unable to apply complex cryptographic system [35].

Due to advancement in technology, it is now necessary to provide end-to-end security. It means that if user uses his/her mobile device for mobile banking then the data transacted are secure at the bank end and not at the user end, thus leaving the data vulnerable to attacks. It was noted that it is difficult to provide end to end security through WAP. The reason is that the data is not encrypted at gateway during the switching of protocol process, which leads to security concern for mobile banking in WAP [36].

In China, mobile communication group introduced the “China Mobile Communication and Information Resources station entities and Internet short Message Gateway Interface Protocol”. It was noted that security is the susceptibility in WAP and that it is safe for the information to be delivered from the gateway to end user but due to accessibility of information for short time on gateway it may be possible for the attacker to access the information [37].

It is identified that users are not usually satisfied from mobile commerce over WAP. The reason is that, problems occur for reasons like low speed, unreliable connection, and high
A research on adaption of WAP services especially for mobile commerce market is in progress in countries like Hong Kong, China, Taiwan i.e. China economic region [38]. In South Africa, there are two technologies used for mobile banking namely WAP and WIG (Wireless Internet Gateway). WIG is a short message service. For South Africa, security and cost are the most important issues in providing the service [39]. In Taiwan, many researches are done in mobile banking and their goal is to develop a much faster service than PC internet banking because it is now realized that mobile banking plays a vital role in customer’s point of view and also from commerce point of view[40].

<table>
<thead>
<tr>
<th>Risks identification related to Mobile banking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security issues</td>
</tr>
<tr>
<td>Password for identification</td>
</tr>
<tr>
<td>SMS based Mobile banking</td>
</tr>
</tbody>
</table>

Table 4: security threads for mobile banking

3.4.2 Authentication Risks and Issues

One of the authentication method used in mobile banking is the login method. However PINS authentication method is an old method and many security issues such as password and id theft were discovered in this method. In such cases, the secret may be revealed and this results in customer’s distrust on the security service company. Bank follows some security mechanisms in mobile banking. While the customers and the banks are bound to each other. This security mechanism is done by identifying the customer’s phone number, SIM card number, pin number etc. Customer likes to use the mobile banking technology because of its mobility as they can access the bank anywhere and in any situation. They can transfer their money from one account to another account faster in a user-friendly environment. And also they can check the current status of their account. But all customers of the bank are not ready to use this service because of some security issues. They are not ready to adopt the mobile banking systems as it brings inconvenience to the users assuming that it cannot prevent direct or indirect attacks.

The security mechanism adopted by the banks face many security issues like being attacked by unauthorized users which is of highest priority in terms of security. If the device gets stolen then the hackers or unauthorized persons may find the password from the log files or saved draft files. Many customers save their password in their mobile or they may keep the password under auto fill settings of the form, this loophole can be easily used by the unauthorized person. Uneducated people are less aware of these issues and thus leading to loss of trust by customers [41].

Authentication Model:
There are two types of services provided to the customer which are as follows:

i. The bank provides the service directly to the customer
ii. Banks share their facility to 3rd party service provider

3.4.3 Bank provides the service directly to the customer architecture
This is a setup which shows the Internet web server, database, application server and firewall at the bank’s side. The above architecture is an example of mobile banking service handled directly by the bank. In this application, server plays an important role to provide services to the customer. The database will be accessed by transactions both from the bank and from mobile device. If a mobile bank customer wishes to process the transaction, for example, transaction of money from one account to another account he/she must first authenticate themselves to the bank server through firewall. And the security application at the server has to verify the user through password or pin number and the server allows the customer to do transactions [40]. In this method, there are some security issues such as server failure, system crash, and malevolent intrusion [42]. These are serious problems and will not make the server come back in normal form. So many banks do not prefer this method.

3.4.4 Banks share their facility to 3rd party service provider

Familiar banks outsource their facility to 3rd party architecture i.e. handling mobile banking customer service to 3rd party service provider. This service provider may lay close to the bank geographically or it may be in other country. They handle the customer through mobile or internet. They are responsible for secure transaction and management of the customer data. This method also has authentication issues as they follow the same authentication method like verifying the pin or password with the database and it also involves 3rd party server. There is no trust [43] in securing the data of customers such as bank account details and customer addresses as they are managed by 3rd party service provider. So customer feels no security to share their password and details to the unknown 3rd party. And also customers need to pay extra charge for their service [44].

This is a list of issues that need to improve by the 3rd party service.
• Network Security & Control
• Parental Controls
• Customer Privacy & Informed permission
• Liability
• Fraud Prevention (or) Authentication
• Interoperability (or) Standardization
• Data Access & Use
• Financial Risks (or) Reward

3.4.5 SMS based Mobile banking

SMS based mobile banking is a convenient and easy way for accessing bank but there are end-to-end security problems. These problems exist in SMS, GPRS protocols and security issues for transaction of money. Today, most of the banks in the world offer SMS based mobile banking. If we take any mobile banking system we can realize that customers also interact with databases, files and important records through mobile phone. Currently South Africa, Bangladesh and some other countries are also doing SMS based mobile banking [4].

Currently in South Africa the standard bank uses WIG and FNB bank uses SMS based approach for mobile banking. In this scenario, the user sends PIN number to the bank’s server and then the server is ready for accepting the requests. This approach is not fully secure because the data is transmitted and the network operator has full access to the data [36].

In Sri Lanka, mobile banking through SMS is gaining more popularity and the reason is that the cost of SMS is very low i.e. 2 Sri Lankan Rupees per SMS which is equal to 0.02 USD. News alert is also one of the popular SMS services in Sri Lanka. Pay Mate is a mobile payment scheme in Sri Lanka. Ezy pay is another scheme of SMS banking through which users can do e-commerce activities. Research is ongoing to secure the SMS banking process [45].

In developing countries like Bangladesh SMS banking is gaining popularity because of low cost and low bandwidth requirement. The main advantages of SMS are the simplicity and easiness to use. Due to plain text property, SMS is not suitable for authentication. So lacking of privacy, integrity and security are the main issues involve in SMS banking [46].

SMS banking is useful for small consumer and for small merchant. SMS banking is also useful for travelers because customer can buy ticket for buses and trains easily and in urgent situations without going to the respective stations [6].

3.4.6 SMS encryption

As default data format for SMS is plaintext. Currently end to end encryption is not available. The only encryption involved at base transceiver station and SMS bank server during transmission. The encryption algorithm used is A5 which is proven to be defenseless [4].

3.4.7 SMS Spoofing Attack

The most dangerous attack in SMS banking is spoofing attack where attacker can send messages on network by manipulating sender’s number. Due to spoofing attack, most of the organizations are not adopting mobile banking through SMS [47].
3.4.8 Virus Attacks in mobile banking

There are more than fifty thousand different types of computer viruses, internet malicious program and Trojans [48]. Software like Trojan horses can easily take up password on the web browser or any cached information on operating system. Malicious codes are written for remote communication [49]. Zeus Trojan targeted mobile bank users. Zitmo has been used by attackers to defect SMS banking. Zeus is commonly used to steal mobile transaction authentication number or password [50].

3.4.9 Risk with Digital Signature

To reduce hardware cost, designer may prefer digital signature. Digital signature is efficient that’s why most companies are interested in digital signature for authentication. It is founded that digital signature is computational intensive. With unsigned values for example date, amount, they differed from transaction to transaction. So a signed template can be used with several unsigned values like date, amount etc [51].

3.5 Biometrics and Mobile Banking

Besides normal way of banking, electronic banking and mobile banking are growing well day by day and shows tremendous improvement but still security threat exists in the system. Providing biometrics for security will make many customers adopt mobile banking. Nowadays bio metrics method is also applied in immigration and visa purpose in European Union [52]. Biometrics method individually identifies the physical behavior of a person. It is impossible to copy, share or forget because of individual has one personal identity [53]. In USA and Europe it is identified that biometrics mechanism is important and to improve level of security. Although technology is advancing day by day and biometrics technology has reached its maturity level; it is still used in limited levels. Media also plays an important role for the popularity of bio metrics methods and awareness among people. Movies like Minority Report and James Bond play an important role for the awareness of bio metrics [54].

Bio metrics play a very important role for the authentication purpose between the physical and electronic identity of customer of mobile banking. There are different types of bio metrics recognition mechanisms especially for the authentication methods. Every person’s biological features are different from the others, so we can say that bio metrics identification is a useful method for authentication because for security purpose it is necessary to identify the authentication uniquely. Some bio metrics methods are voice recognition, hand based recognition, finger print recognition, face recognition etc. but the most suitable and less data consumer in database for storage purpose and most users friendly and easy method is finger print recognition. Research is ongoing in the finger print technology so many different types of sensors are developed. In 1998, Siemens PSE and Trio data developed the first mobile phone which included a sensor [8].

A general bio metrics mechanism is shown below:
3.5.1 Vision for Secure Mobile bank transaction:

<table>
<thead>
<tr>
<th>Adoption of mobile banking</th>
<th>Vision</th>
</tr>
</thead>
</table>
| Secure payment transaction needs | • Secure identification method  
• Enrollment of bio metrics method like fingerprint  
• Minimizing the fraud in mobile banking  
• Privacy  
• Data integrity  
• Self-efficiency  
• Preventing virus Attacks |

Table 5: Improving electronic banking Security with Bio metrics method
4 INTERVIEW PHASE

After doing Literature Review and finding the current security issues in mobile banking, it is realized that the expertise of company is involved and by conducting interview from their expertise found how to improve authentication security level in mobile banking.

4.1 The Interviews

There are mainly three types of Interviews:

i. Structured interview

Structured interview is about asking the questions in particular time and the answers are given by expertise. In this case, the answer can be categorized in the form of good, average and very well. Structured interview is about asking the questions in particular time and the answers are given by expertise. In this case the answer can be categorized in the form of good, average and very well. In structured interview the questions are very specific. Specific objectives are determined through structured interview. In structured interview the same questions are asked from all candidates. Normally a rating scale is used for question and answer session [55].

ii. Semi Structured interview

Semi Structure interview consists of an open ended questions based on research area. In Semi Structure interview the topic is discussed in more detail which helps the researchers to get and take advantage from the expertise in research area. Qualitative phenomena measurement often collected by using semi structured interviews. In semi structured interview data from interviews was triangulated in form of fault determination and their observation. Semi structured interview is also called focus interview. The activities involved in semi structured interview are scheduling, collecting information, preparing interview guide, discussion/meeting, summery writing, transcribing banking [56]. The authors conducted semi structured interviews. By semi structured interview the authors determined what the benefits of mobile banking are. Authors also determined about current mobile banking authentication and its effects on customers. Authors determined importance of finger print as authentication method in mobile.

iii. Unstructured interview

Unstructured interview have a very little structure and make questions based on previous session. In unstructured interview candidate can be asked by variety of questions. A standardized rating scale is not required in unstructured interview. Low validity and reliability involved in unstructured interview [57].

4.2 Industrial Interviews

More efficient information has consumed by face to face meeting/interviews. Based on interview, it is easy for the author to design his framework for his research so it is necessary to contact the person related to the research area [58]. Semi Structured interviews were conducted from the relevant expert customers so that important information is collected to do the thesis in good way.
4.3 Selection of Interview Subject

Peoples who are involved with the security issues of mobile banking and designing phase of mobile banking applications were considered here to get the precise and useful information from them. Interviews were conducted from the expert persons who have at least 2 years’ experience related to the mobile banking or designing phase of mobile banking applications. More interviews are conducted on the basis of security issues and the ways to reduce the fraud activities. Broad aspects of questions were asked from the expert peoples.

4.4 Interviewing

Each interview was conducted in duration of 35 to 40 minutes from the expert peoples. Research question is designed before the interview. Interview was recorded and important points were noted. Finally, the results were analyzed and more information about the security issues of mobile banking was found.

4.4.1 Designing Questions for Interview

Section A: The general questions about mobile banking and its impact on customers, adoption of mobile banking, its relationship with e-commerce and other applications like mobile payment etc.

Section B: The second section is about the role of mobile companies for developing and designing secure handset for the sensitive services like mobile banking, secure transaction, secure authorized process etc.

Section C: Presenting expert views about how to make secure transaction of mobile payment through mobile handset. Finding secure authorize method and the role of biometric method in mobile handset.

4.4.2 Analysis of the Interviews and Literature Review

In this section, analysis of the industrial interviews and Literature Review are presented. Security issues were found from different databases of Literature Review. Bank interviews help us in order to overcome security issues for the transaction of payment system doing mobile banking and to develop trustworthy mobile banking for customers. Another advantage of industrial interviews is to figure out the views of the expert person to make mobile banking more secure so that peoples can easily make their e-commerce activities.

<table>
<thead>
<tr>
<th>Factors</th>
<th>Current mobile banking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliability</td>
<td>• Customer does not want to wait. So the slow speed can affect the transaction doing mobile payment.</td>
</tr>
</tbody>
</table>
| Security | • If message is lost then transaction will fail  
• SMS cannot be encrypted it is in plain text. So hacker can hack the SMS. |
Customer satisfaction
- Customer mostly prefers internet banking as compared to mobile banking.
- Customer does not transfer large amount through mobile services, they hesitate due to security threats.

Fraud
- Banking security is improving day by day but still fraud occurs. Secure system is needed to minimize fraud chances.

Self-Efficiency
- As no face to face contact occurs in mobile banking. Due to security risks involved in mobile banking, customer satisfaction and self-efficiency is low for the transaction of payment through mobile device.

Table 6: Current mobile banking system

<table>
<thead>
<tr>
<th>Factors</th>
<th>Bio metric mobile banking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security threats</td>
<td>• Secure Authentication method is needed.</td>
</tr>
<tr>
<td></td>
<td>• By bio metrics mechanism, fraud activities can be minimized and security level can be</td>
</tr>
<tr>
<td></td>
<td>improved. For more security encryption algorithm is used.</td>
</tr>
<tr>
<td>Customer satisfaction</td>
<td>• Customer satisfaction will be increased by the finger print mechanism because fraud will</td>
</tr>
<tr>
<td></td>
<td>be minimized.</td>
</tr>
<tr>
<td></td>
<td>• The transferring of money is well secured because finger print increases security level.</td>
</tr>
<tr>
<td>Easy access</td>
<td>• Easy access to bank service.</td>
</tr>
<tr>
<td></td>
<td>• Any time availability and easy use.</td>
</tr>
<tr>
<td>Time consuming</td>
<td>• Less time consuming because of easy access to bank services.</td>
</tr>
<tr>
<td>Authorization</td>
<td>• Authentication is an important factor because it is necessary to know that the authorized</td>
</tr>
<tr>
<td></td>
<td>customers are using mobile banking services.</td>
</tr>
<tr>
<td>Self-efficiency</td>
<td>• Through finger print authentication customer self-efficiency gets increased. The reason is</td>
</tr>
<tr>
<td></td>
<td>that customers are satisfied due to ensuring that direct authorized person is involved.</td>
</tr>
</tbody>
</table>


| Trust | • As finger print is unique it cannot be stored. The customer trust is more on finger print authentication compared to ordinary login system. |

Table 7: Bio metric Mobile banking
5 BIOMETRICS MOBILE BANKING SYSTEM

5.1 Proposed Bio metric mechanism

5.1.1 Bio-Metric

It consists of physiological and behavioral characteristics; it helps to find the uniqueness between the human beings. These characteristics may be related to shape, structure, color or behavior of person. Any one of these characteristics are captured by biometric method and stored in a computer. Later this data is stored and used for identifying the person.

5.1.2 Proposed Mechanism

This thesis mainly focuses on how to enhance the security in mobile banking. The authentication process is one of the important parts of the whole chain, in terms of security perspectives; bio-metric is included for the authentication in mobile banking. RF (Radio Frequency) imaging finger print technology helps and keeps the system more secure. This RF image scanner will find the inner layer of live skin as well as it prevents the adhesive film (fake finger print) so it will give an accurate image. Through analysis of LR and interviews, we found that security can be improved by biometric system. Finger print system is more suitable, secure and takes less data storage as compared to other bio metrics mechanism [59].

In face biometrics mechanism, the template takes around 1300bytes and in voice biometrics mechanism, the template takes around 6000bytes but compared to finger print biometric mechanism template which takes only 256 bytes are expensive. In this chapter, we will show a model of bank system with finger print mechanism. Finger print method is gaining popularity in every organization and existing systems are replaced by bio metric system. Especially for authentication methods, finger print mechanism is used. Due to security and privacy bio metric system is adopted in many organizations like airport, passport office, immigration offices etc [60].

5.1.3 Bio metric Authentication method in Mobile banking Model

![Figure 6: The finger print method for authentication in mobile banking](image)

* Finger print is unique.
* Finger print can be encrypted.
* For high security PKI public key is used.
* In raw state finger print is unable to store.
* Supporting software are Sun -Java Wireless tool kit.
* Finger Print cannot be copied or shared.
* RF[Radio Frequency] prevent adhesive and accept live skin
* sensor have capacitance plates. By electric charge it will be able to make finger print pattern.
5.1.4 Proposed Bio metric Mobile Banking System diagram

There are two types of users (1) registered user (2) new users. The registered users will directly go to login form while the new users will go to registration form.

i. RF scanning is used because through RF scanning, it is possible to differentiate between living cells and dead or copy cells. So to ensure that the authorized person is using mobile banking service, RF Scanning technology is used in bio metric mobile banking system [59].

ii. After verification of data, the customer will be able to access the database through web server.

iii. If the finger print matches to database then customer will be able to start mobile banking services through mobile handset.

iv. For additional security LDAP server is used. If first finger print authentication is not found in database then it will be checked in LDAP server for more verification.

Figure 7: Flowchart of proposed bio metric mobile banking system
v. New users have to register any three finger print in database and also need to fill registration form.

vi. If the finger print of the bank customer is registered successfully then customer will be able to use mobile bank services.

5.1.5 Biometric Fingerprint Scanner device

For secure authentication purposes the author proposed finger print scanner device.

![Biometric Finger Print Scanner](image)

**Figure 8: Proposed Finger Print Scanner**

The authors propose a new model finger Scanner device in mobile banking as shown below. Biometric finger print scanner device will help mobile companies to design mobile with implementation of finger print mechanism. The mobile device manufacturers are required to design mobile device with supporting bio metric finger print scanner device.

The proposed Finger Print scanner device phenomena:

i. Mobile manufacturing companies will make the biometric scanner device with mobile hand set. The mobile customer will used it for authentication purposes.

ii. The Bio metric finger print scanner device will replace the traditional way which secures the information like PIN (Personal identification number) which is considered as a risk [61].

iii. For capturing finger print, there will be a sensor. Because nowadays hardware platforms are supporting different types of sensor interfaces to capture the data [62].

iv. After capturing finger print, the data will be transmitted through internet. And the data can be accessed through bank server.

v. Comparing the finger print in the database at server end it will be confirmed whether or not an authorized person is accessing mobile banking system.

vi. The finger print scanner device can be attached to mobile phone though Port.

vii. Privacy and trust level will be high because biometric cannot be updated or revoked [63].

viii. Among all bio metric systems, finger print system is more popular because of low data storage capacity as compared to other biometric features like voice and face recognition etc[64].

ix. In Bio metric mechanism, finger print scanner is widely used in many organizations especially, like national border control, passport offices, and Airports etc. Now to make mobile payment and to access mobile services it is necessary to integrate such bio metric mechanisms in bank sector for security purposes [60].

x. Chargeable low cost battery will be used for charging the finger print device.

xi. Finger print device have sensor. The sensor has Capacitance plate. The capacitance has the ability to hold the electrical charge. By electrical charge it will be able to make finger print pattern [65].
5.2 Mobile banking mechanism through Finger Print

The following are the steps for performing bio metric mobile banking through finger print mechanism. After attaching Finger Print scanner, the customer will be able to perform mobile banking services through handset mobile phone.

Step 1: Enter login Page:
Customer need to enter account number.

Step2: New User
If the customer is a new user then select the new user button as shown in figure.

Step 3: Register Form
New customer has to fill the following requirements as shown in the figure. After entering all information the customer has to click next button.

Step 4: Selecting Sample Finger Print.
Customer can select any three fingers as sample. Each finger is denoted from left to right (s0 to s9), if the customer selects the check box for 3 samples finger then click next.
i. The process which statistically gives you best possible template called consolidation. According to Statistical research, it was found that the consolidation of three finger template produce high quality enrolled template [66].

ii. Finger print software does not store the digital image [66]

Step5: Scanning Processes
With the help of finger scanner device, mobile handset gets three samples as shown in figure. These samples are stored in bank server with appropriate account holder. In case of cut, burn, damage of one finger the other finger print data will still serve as a unique identifier [26].

i. Finger print cannot be copied or shared.

ii. Minutiae extractions mean extracting features from Fingerprint and store in the database [67]. For authentication purposes finger print is captured by using biometric algorithm and stored in server for enrolment. This algorithm measures 40 or more data point for each finger print and encrypted as a digital certificate. Different type’s algorithms techniques are available to prevent hackers attack, one of the techniques is the sample image has changed in different manner. For e.g.: “It may be considered that this technique is sampling in a polar coordinate space. Under this approach, the sampling resolutions are the distance between the concentric circles and the sampling interval within the circumference of the circles” [68] if mathematical representation of finger print is not matching then actual finger is not using for authentication purposes.

Step6: Authorize your Finger Print for registered customers:
If the customer has selected “yes” option for checking, this page will appear for checking the customer sample with saved sample. Customer have to scan their finger print with the help of the device and click the submit button for confirmation.

Finger print is present for matching in the database record. Every time new finger print is compared to the stored finger print [26]. Based on Minutiae the customer template is compared and if it matches then further processing starts [67].

Step7: Progressing for confirmation
Nowadays servers are capable of processing finger print data at a speed of 2000 record per second [26].
Step 8: Confirm Page
When finger print matches the database the confirmation message will be displayed on the mobile screen.

Step 9: Confirmation page
When the database server authenticates the user then confirmation message will be displayed on mobile cell phone screen.

For authentication purposes and to secure customer data at server end additional server called as Server LDAP authentication is used [69].

5.3 LDAP (Lightweight Directory Access Protocol)
working mechanism for security purposes

In LDAP, the client sends the query packet through TCP/IP to the server. The server confirms the identifier on LDAP Directory Information Tree (DIT) which is stored on LDAP server. When the result is found, it is sent back to client. In case of result not found then query will be sent to another LDAP server. This LDAP verify the data in tree model structure method. So this is highly secure [69].

TCP/IP network

LDAP client  LDAP server

LDAP protocol

Figure 9: Working Mechanism of LDAP
LDAP authentication has many advantages like centralized usage, privileges, management, and storage of user information and user accounts [69].

Proposed System Architecture process:

Here mobile is linked with server having different IP addresses. The mechanism for authentication is located on web login form which is used for granting permission to a user. This permit will be on LDAP server or database web server. Secure Socket Layer (SSL) protocol is used for transaction or communication for security purposes.

5.4 Authentication and authorization mechanism

In this mechanism, account number and finger print are used. If account number and finger print matches with those in bank database server then customer can access the bank services. In order to access the bank services, it is important for the customer should authenticate.
Access to bank services based on bio metric method (Finger Print mechanism)

Step1: Customer requests to access bank account.
Step2: Request is accepted and the server requires finger print from the customer.
Step3: Customer has disclosed finger print and account number to the server
Step4: Matching account number and finger print sample and verify with N samples in database. When finger print matches, connection is established between the customer and bank server.
6  WORKSHOP

For validation purposes, the authors conducted a workshop about “Bio metric Mobile Banking”. The agenda of the workshop were to present the proposed Bio Metric Mobile Design to experts for evaluation and also to take useful suggestions.

6.1  An Overview

This workshop took place in BTH campus and about 16 potential future users attended the workshop. The participants included academic computer science teachers, PhD students and Master level computer science student.

The workshop participants actively participated in the discussion session and also gave their suggestions. The audience gave suggestions about “proposed bio metric banking”. The participants discussed about banking system and bio metric system. Participants agreed that by bio metric method security will be increased. They also discussed the current risks in mobile banking and gave suggestions about the proposed finger print scanner device and its roll in mobile banking.

6.2  Aim and Objectives

The major goal of the workshop is to take feedback from the participants and present it as result.

The main aim of workshop is

i. To get feedback and useful suggestions by presenting proposed bio metrics mobile banking. First the authors discuss the customer distrust about mobile banking and then explain current security issues in mobile banking. After that they were proposed the bio metric Mobile banking system.

ii. Taking the feedback from the participants at the end of workshop. Some questions were distributed among the participants. And also took response of the audience.

iii. To investigate about current mobile banking and biometric mobile banking.

6.3  Participants

There were 16 participants in total

6.4  Activities

6.4.1 Welcome and Introduction

The authors gave warm welcome to all participants. Then authors introduced themselves. Also authors described the thesis work which includes introduction of the thesis.

6.4.2 Presentation

The authors started the presentation from the background of the thesis, then the research area was and presented the proposed bio metric mobile banking. In this presentation, the following were presented in detail

i. Security issues in current mobile banking service.

ii. Recent mobile banking mechanism in different countries.
iii. Proposed bio metric device.
iv. Proposed bio metric mobile banking mechanism.

During the presentation participants took note of important points. After a presentation of 50 minutes, half an hour was given to the participants for discussion and asking questions. At the end, questionnaire was distributed among the participants to determine the evaluation about the proposed mechanism.

6.4.3 Discussion Session

The participants asked some important questions during the presentation. But at the end the authors gave additional time to participants for discussion.

Some important key points of the discussion are presented in the following table:

<table>
<thead>
<tr>
<th>Discussion points in the workshop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current mobile banking system and customer’s attitude for transaction of money through mobile device.</td>
</tr>
<tr>
<td>Authentication for mobile banking. Ensuring that authorized person is using mobile device for mobile banking.</td>
</tr>
<tr>
<td>Security issues in SMS banking.</td>
</tr>
<tr>
<td>Proposed secure authentication method finger print in mobile banking.</td>
</tr>
<tr>
<td>Simple identification number (ID) and password methods for mobile banking and security threads for mobile banking.</td>
</tr>
<tr>
<td>Mobile banking is easy and convenient way for customers.</td>
</tr>
<tr>
<td>Customer will feel secure of their money transaction because finger print is unique for every person.</td>
</tr>
<tr>
<td>Participants also discuss about SMS banking. They said SMS banking is easy and convenient method but only for information or account details display.</td>
</tr>
<tr>
<td>Some participants suggest that comparative study of other bio metric system can be conducted, and further modification can be made to the proposed system.</td>
</tr>
<tr>
<td>Need more study about setup network between mobile and bank system?</td>
</tr>
<tr>
<td>Need mechanism to differentiate between living and dead cells of finger. So that only authorized person will able to do mobile banking.</td>
</tr>
</tbody>
</table>

| Table 8: Key points of discussion |

During the discussion session, the participants explored their views about proposed bio metric mobile banking and specially the proposed finger print scanner device used in mobile banking.

The Questions which rose during the workshop are given below:

i. Which type of mechanism you proposed so that it should be ensured that authorized persons is doing mobile banking through finger print device?
ii. How do you justify that your method is better than current mobile banking mechanism?
iii. How will it be useful for supermarket when customer wants to buy items?
iv. Why did the authors select finger print mechanism? Why did you not select other bio metric mechanism like voice, face recognition etc?
v. Is there any possibility that the finger print device can be used instead of ATM card? Because ATM is also not secure. ATM can be swap the machine reader and money can be transfer from customer account to another account.
vi. How the finger print differentiate between live and dead cells of finger. Is there any type of advance technology included in the finger print device?
The participants actively participated in the workshop. They exposed their views. They discussed lot about current mobile banking and proposed bio metric mobile banking. They also give us useful suggestions to improve work. The discussion session was about 40 minutes.

### 6.5 Questionnaire

At the end of discussion, questionnaire was distributed among participants. The questionnaire consisted of 10 questions. The questionnaire was designed according to Likert Scale [70]. The participants were given 15 minutes to fill the questionnaire. The workshop questionnaire is shown in Appendix B.

### 6.6 Feedback

From the discussion, useful suggestions given by participants and from the results of the questionnaire it was found that the workshop presentation is very informative and interesting.

At the end, the participants provided their perception and appreciated the bio metric mobile banking as:

i. By finger print mechanism it will be sure that authorized person is using the mobile handset for mobile bank services.

ii. Authentication is one of the important factors of security.

iii. Mobile banking through mobile handset is easy and can operate from anywhere.

iv. It will be more advantage if the whole system is secured from mobile handset to access of the bank server.

v. Due to low storage capacity, slow speed of processing, hackers can take advantage and be able to attack customer’s personal data. Due to Finger print scanner, it is possible to prevent the attackers because it is one way mechanism and cannot be copied.

vi. Also participants discussed about money transaction through mobile phone. Some participants said that they would like to transfer money through mobile handset if it is fully secure.

vii. Also participants discuss the proposed finger print scanner that it seems to be good choice for ease of use. After answering the Questionnaire then authors will be able to express the result. The following table shows the participants views about proposed bio metric mobile banking:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Number of Questions</th>
<th>Strong Agree</th>
<th>Agree</th>
<th>Neutral</th>
<th>Disagree</th>
<th>Strong Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ease of use mobile banking</td>
<td>5</td>
<td>90%</td>
<td>10%</td>
<td>Nil</td>
<td>Nil</td>
<td>Nil</td>
</tr>
<tr>
<td>Customer Satisfaction</td>
<td>3</td>
<td>10%</td>
<td>70%</td>
<td>20%</td>
<td>Nil</td>
<td>Nil</td>
</tr>
<tr>
<td>Fraud reduction</td>
<td>4</td>
<td>10%</td>
<td>60%</td>
<td>20%</td>
<td>10%</td>
<td>Nil</td>
</tr>
<tr>
<td>Suitable authentication</td>
<td>1</td>
<td>50%</td>
<td>30%</td>
<td>Nil</td>
<td>10%</td>
<td>10%</td>
</tr>
<tr>
<td>Trust</td>
<td>6</td>
<td>40%</td>
<td>40%</td>
<td>Nil</td>
<td>10%</td>
<td>10%</td>
</tr>
<tr>
<td>Safety</td>
<td>7</td>
<td>50%</td>
<td>30%</td>
<td>10%</td>
<td>10%</td>
<td>Nil</td>
</tr>
</tbody>
</table>
Table 9: Percentage of criteria of the proposed bio metric mobile banking

<table>
<thead>
<tr>
<th>Criteria</th>
<th>8</th>
<th>60%</th>
<th>30%</th>
<th>10%</th>
<th>Nil</th>
<th>Nil</th>
</tr>
</thead>
<tbody>
<tr>
<td>Easy way of use for service</td>
<td>2</td>
<td>40%</td>
<td>40%</td>
<td>20%</td>
<td>Nil</td>
<td>Nil</td>
</tr>
<tr>
<td>Security</td>
<td>11</td>
<td>90%</td>
<td>10%</td>
<td>Nil</td>
<td>Nil</td>
<td>Nil</td>
</tr>
<tr>
<td>Self-Efficiency</td>
<td>12</td>
<td>70%</td>
<td>20%</td>
<td>10%</td>
<td>Nil</td>
<td>Nil</td>
</tr>
</tbody>
</table>

The above table shows the percentage of different criteria of the proposed bio metric mobile banking system. The percentage shows the participant’s answers about proposed bio metric banking that how much they give value to a particular criterion.

Figure 12: Percentage of Response of Questionnaire analysis

Almost 90% of participants strongly agreed that finger print mechanism is a very good choice for ease of use. And the remaining 10% agreed that finger print mechanism is a good choice. Also participants gave better response to easy way of use; customer satisfaction will be increased through finger print scanner device. Some customers gave negative response, as trust is related to personal feeling but 40% of participants agree that trust will be increased because security level is increased.

Participants were strongly agree about good choice for “ease of use” and increase “Self efficiency” for authentication. The following chart shows that 90% ease of use for mobile banking will be increased by finger print mechanism are used for authentication. Participants were agree that as no face to face contact occurs in mobile banking so self-efficiency will increase by finger print mechanism.
Participants also discussed that security will be increases due to finger print authentication. The participants discussed that different type of algorithms, encryption purposes exist for biometric authentication methods. So they preferred finger print on other mobile banking mechanism like SMS banking, Login & Password etc.

After the workshop authors concluded that customer trust is effected by security issues. Mostly customer distrust on mobile banking due to security. The following chart shows that finger print is suitable authentication method for mobile bank customers.
Figure 15: Trust and Security analysis in workshop
7 ANALYSIS PHASE

From LR, interviews the authors founded many factors due to which customer distrust on mobile banking. The authors founded that customer distrust on mobile banking due to security reason. Authentication is one of the main parts of security. In workshop authors proposed finger print authentication method for mobile banking.

7.1 Trust in mobile banking

As from (section 2, Background) many factors were founded that can effect customer trust for mobile banking. For example convince, cost, reliability, technological failure, Technical failure, virus attack, Security issues etc. As no face to face contact is there so it is realized that trust is an important factor for mobile banking. In (section 2.1.2) it is explained that Trustworthy system is needed for mobile banking [26]. Security is founded main reason for customer distrust on mobile banking [4].

7.2 Security issues in mobile banking

In (section 2.1.5) it is explained that Authentication is the important factor for the trustful and secure use of mobile devices for accessing mobile banking services [32]. By LR authors founded many security issues which are briefly explained in chapter 3. For this purposes the authors make basic model for mobile bank transaction and included all security risks. In (section 3.3) Mobile bank transaction service model shows that many security risks are involved to prevent customer from huge transaction services. In (section 3.4.1) it is explained that the data is not encrypted at gateway during the switching of protocol process, which leads to security concern for mobile banking in WAP [37]. Similarly in (section 3.4.4) “Bank shares their facility to 3rd party” so there are also security risks in “Bank share their facility to customers”. Customer feels no security as he/she has to share their password and details to the unknown 3rd party [44]. SMS banking is one of the popular services in Asia countries because of low rate. Bangladesh and Seri Lanka SMS banking gaining more attention and popularity due to their low cost [45][46]. Main problem in SMS banking is that no end-to-end encryption is available. In (Section 3.4.6) it is explained that the only encryption involved at base transceiver station and SMS bank server during transmission. The encryption algorithm used is A5 which is proven to be defenseless [4]. In (Section 3.4.7) it explained that SMS spoofing attack is also security issue for mobile banking [47]. (Section 3.4.8) it is explained that virus attack in mobile banking. There is more than 50 thousand computer viruses. Software like Trojan horses can easily take up password on the web browser or any cached information on operating system. Malicious codes are written for remote communication. In (section 3.4.9) it is explained that security risks were also founded in digital signature. Because unsigned values for example date, amount, they differed from transaction to transaction. A signed template can be used with several unsigned values like date, amount etc [51].

7.3 Secure authentication method

By LR and interview it is founded that security can be increase by biometrics authentication method. In (section 3.4.10) it is explained that Biometrics method individually identifies the physical behavior of a person. It is impossible to copy, share or forget because of individual has one personal identity [53]. In interview phase it is founded that customer satisfaction are effected by security threads in mobile banking. In (Section 4.4.2) it is discussed that participants of interview were agree that fraud chances are high in current mobile banking
due to security risks. The interview participants were also agree that self-efficiency will be increase by finger print authentication method. According to them fraud chances will be reduced. The participants were agree that finger print is unique and more suitable as compare to other biometric mechanism like voice, face recognition etc. interview participants were agree that bank revenue will be increased by secure finger print authentication.

7.4 Proposed finger print authentication mechanism

From LR and interviews it is founded that finger print is more suitable and user friendly as compare to other biometric mechanism voice, face recognition etc. (Section 5.1.2) explained that finger print template takes 256 bytes data which is less as compare for template voice recognition and voice recognition [60]. This RF (Radio Frequency) image scanner will find the inner layer of live skin as well as it prevents the adhesive film (fake finger print) so it will give an accurate image [59]. (Section 5.1.3) explained about finger print authentication model. (Section 5.1.4) proposed biometric mobile banking system diagram. Section (5.1.5) the author proposed biometric finger print device. Biometric finger print scanner device will help mobile companies to design mobile with implementation of finger print mechanism. The authors also explained finger print device phenomena. (Section 5.2) Finger print mechanism that is used for authentication purposes. According to Statistical research, it was found that the consolidation of three finger template produce high quality enrolled template [66]. Finger print cannot be copied or shared. Finger print is digitized, secure algorithm and encryption can be applied on it. Different type’s algorithms techniques are available to prevent hackers attack, one of the techniques is the sample image has changed in different manner. For example “It may be considered that this technique is sampling in a polar coordinate space. Under this approach, the sampling resolutions are the distance between the concentric circles and the sampling interval within the circumference of the circles” [68] if mathematical representation of finger print is not matching then actual finger is not using for authentication purposes. For additional security LDAP server is used. If first finger print authentication is not found in database then it will be checked in LDAP server for more verification [69].

7.5 Workshop

As in (section 6.4.2) it is discussed that agenda of workshop is to present:

i. Trust and Security issues in current mobile banking service.
ii. Recent mobile banking mechanism in different countries.
iii. Security for authentication can be improved by finger print mechanism.
iv. Proposed bio metric mobile banking mechanism.

At the end questionnaire is distributed among workshop participants. At end they also give suggestions. From discussion session it is observed that security level, self-satisfaction will be improve by finger print mechanism. At end questionnaire were distributed among participants. The evaluation of questionnaire was done according to Likert Scale. From participant’s discussion and answering of questionnaire it was founded that finger print can improve security as well as customer trust for mobile banking. They are advantages for bank sector in term of revenue. Workshop Participants prefer finger print for authentication purposes as compare to login, PIN, user name, password etc.
8 VALIDITY

Research validity [71] plays an important role because it shows the accuracy and trustworthiness of the outcome.

At the beginning of the thesis the security issues and the risks which customer face when they are doing current mobile banking was explained.

Validity Threats
There are four criteria for validity:
   i. Credibility
   ii. Transferability
   iii. Dependability
   iv. objectivity

The Author explains the above validity threads regarding to the thesis.

8.1 Credibility

Credibility means internal validity. According to Harvey Russell Bernard, the Credibility result depends on research work. Good measurement is the key and power of credibility for a research. In this thesis, the participants shows interest and appreciate the research work - Credibility means internal validity [72].

In the beginning, qualitative research was used because the research was started by conducting literature reviews. Many articles were found during searching but Author chose only the selected documents which are related to current issues in mobile banking. Keep in mind the research work and time framework to minimize the risks. For this purposes the authors also conducted interviews for their research work. Authors made their interviews with bank managers and academic staff. The interviews were conducted with Swedbank Manager and IT staff of Swedbank Ronneby Sweden. First the Author explains the whole thesis mechanism which includes security issues in mobile banking and then explains our proposed bio metric mechanism for mobile banking. The bank manager and IT staff share their knowledge about mobile banking and the advantages of bio metric mechanism. The authors also did interviews with academic staff from BTH Karlskrona. The remaining two interviews with bank managers were conducted through Skype.

Then the author proposed a bio metric mobile banking systems which contain the designing of finger print scanner device for authentication and mobile banking mechanism.

For proposed mechanism, the authors conducted workshop. In workshop academic experts, PhD students and Master level students participated. The participants were the one who have been expertise related to mobile banking. After the presentation, the participants had a detailed discussion. At the end, Questionnaire was distributed among the participants. The main aim of workshop is to find out the evaluation of the proposed mechanism. Our result is depending on the proposed mechanism and the answers of participants attended the workshop.

8.2 Transferability
The external validity is called transferability [71]. Selection of wrong people’s views can also affect the research work. In order to minimize the threads the authors selected bank staff and academic staff for interview. The reason is that they give us useful suggestions and aware about mobile bank mechanism and its effect on customers.

Various department experts were participated in the workshop. But all are related to computer science fields. The participants were from Software Engineering, Electrical Engineering, and Computer Sciences.

The participants of the workshop show their interest in research field of mobile banking and bio metric mechanism. Most of the participants agree that security level will be increase by finger print method for authentication. The participants also show their interest in bio metric banking and suggest that bio metric can play a vital role for security purposes in any organization.

The participants say that the proposed bio metric mechanism can be implemented in any country and it will help many companies to design secure devices. They said that the bank revenue will be gradually increased by using such secure authentication methods. The participants also talked about some limitation of finger print authentication. For example if whole hand burn then customer cannot be able to use finger print for authentication purposes.

8.3 Dependability

Dependability shows the reliability of the work. Dependability explains and identifies what will be the benefit of the research and also will explain the variation in the proposed research field [71].

For this purpose, the Author had identified the current security issues in mobile banking and proposed secure authentication method for bio metric mobile banking. In the workshop most of the participants were aware about technical terminologies but some participants asked questions about technical terminology related to bank system and different bio metrics methods. The participants also discussed about the reliable system. And they said that bio metric mechanism is more reliable than any other mechanism.

8.4 Objectivity

The objectivity means the validity of the outcome of proposed result. The conformity of the research is called objectivity. The authors conduct study of current mobile banking system [71]. Then find out the problems facing by the customers and also the risks related to the money transaction. It is briefly explained in chapter 1, 2 and 3. The bio metric method was explained in chapter 3. The product result was presented before the experts who attended the workshop.

The positive feedback provided by workshop participants shows that secure authentication is the need for current mobile banking and security authentication can be improved by bio metric method which is finger print and mostly acceptable.

It is also observed that customer trust can be increased if secure authentication method is used for mobile bank services.
9 EPILOGUE

9.1 Conclusion

In this thesis, we introduced and validated design method for mobile banking by using biometrics to improve security, trust and ease of access. First we identified the strength and weakness of the different authentication methods. This can be done by conducting Literature Review and interviews from professionals and bank experts.

In first step, it was observed that there is lagging of security and there is no formal authentication between the customer and the bank. Hackers can easily cyberpunk and there is no assurance the bank authenticates the authorized person. For this reason bio metric authentication method was introduced to improve the security.

In second step the method based on designing was defined by using both strengths and weaknesses of current authentication mechanism. Much of the design process was based on suggestion from professionals and bank experts.

In third step the design method was validated by conducting workshop. The authors introduced biometric finger print design for authentication and the identified minimum requirements are selected for conducting workshop as time was a constraint.

This thesis fulfills the gap of authentication between the customer and the bank. The result shows that the biometric design increases the security level between the user and bank. The security will also increase the bank revenue.

Fraud can be minimized by bio metric mechanisms; especially finger print is suitable and secure method for the authentication of customer. The author designed the mobile handset and proposed a future device through which customer can scan finger print. Due to uniqueness of finger print it assured that authorized customer is making use of mobile banking. As data is sensitive at server level of bank system we propose System Architecture process. In this way data will be secure for the customer doing mobile banking services from end to end.

9.2 Answers to the Research Questions

Research Question1: Why does customer not trust on Current Mobile Bank Transactions?

For Research Question1: The authors identified Trust factors by Literature Review. Section 2.1.1 Trust in mobile banking described factors that customer did not trust on mobile banking. Then find out that security is the main issue for customer distrust.

Research Question2: What are the security issues in current mobile banking?

By LR security issues and the risks are identified when customer wants to do mobile banking. For this purposes authors took help from Literature Review. The authors made a basic model for mobile bank transaction and add security issues in the model. The authors explain all security issues in detail. See section 3.3 and section 3.4.

Research Question3: Which kind of authentication method is more suitable for the customer doing mobile banking services?

The authors identified from LR that by bio metric the security level is increased. For this purposes the authors identified suitable bio metric (finger print) mechanism. As finger print is uniquely identifying the person identity so that’s why authors think that finger print will
play an important role for bank authentication. The authors proposed a bio metric mobile banking system. It is observed that authentication method through finger print is more trustful as compared to other type of mobile banking mechanism. The authors also show mobile bank transaction by finger print mechanism. In supporting LR authors also conducted interviews from banks and academic experts. This is explained in detail in chapter 4 and 5.

**Research Question 4:** How bio metrics can play an important role for secure authentication in mobile banking?

The Author explained the advantage of bio metric mechanism especially for finger print. It is observed that customer satisfaction, trust level increased by finger print mechanism in mobile banking. The Author also explains the latest technology like RF (Radio Frequency) role in finger print scanner device. The details are provided in chapter 5 and chapter 6.

### 9.3 Future Work

Further this special finger print device can be improved to provide the features which enables effective communication with any other device like ATM machines, shopping, ticket booking, bank transactions and also for user identification. As a future work, it has been planned to implement the cloud technology in bank sector. This ensures secure authentication thereby increasing the bank revenue and reducing the networking problems which arise mainly due to congestion and unauthenticated sessions. Further study in the encryption techniques that can be used along with this system will increase security in mobile banking to a greater extent. Integration of other bio metric mechanisms along with this system could also be done with some research in terms of cost, effectiveness and feasibility might increase the security by folds.
REFERENCES


Communications of the IBIM.


[40] Dian Yan Liou, “Four-scenario analysis for mobile banking development


10  **APPENDIX B**

10.1  **Interview Questions**

**General Question:**

1) Do you think that current mobile handset has secure authentication for the mobile payment?
2) How do you think people react toward transaction through mobile handset?
3) Do you think mobile banking improve the bank revenue?
4) Do you think customer expecting more security for regular transaction using mobile device?
5) Do business people give more importance for authentications to ensure end to end users?
6) Do you think authentication is important to ensure end to end user?
7) Do you think secure mobile banking services can improve trust between buyer and seller especially in E-commerce systems?
8) What factors can be affected in mobile handset when the customer doing mobile payment transaction?
9) Do you think using mobile banking will be more user friendly as compare to internet banking?
10) What do you think disclosing of personal information can help the hacker to access banking account through mobile? Like losing mobile handset and SIM (containing information about customer detail)
11) How you come across the security issue of mobile payment transaction in e-commerce when customer selling or purchasing items using mobile handset.

**Bio-metrics Question:**

1) Do you think bio metrics method can improve the security level?
2) There is different type of bio metrics methods? Which one is your preference and why
3) Finger print
4) Eye trace
5) Voice recognizer
6) Face recognize
7) Do you think bio metric mechanism can be embedded in all mobile handset?
8) Do you think that Bio metrics mobile banking will be able the customer accomplish the mobile banking services task very quickly?
Transcribed Interviews

Interview 1

Name: Dr. Jeanette Eriksson
Email address: Jeanette.eriksson@bth.se
Contact information: 0455-385870
Dept. of Computer Science
Company: Blekinge Tekniska Högskola
Date: 10/June/2011
Start and End time: 10:00A: M to 10:25 A: M

The contacted person for interview was Mrs Jeanette Eriksson, currently working as a senior academic Lecturer in computer science department in bth campus Sweden. The research area of Mrs. Jeanette Eriksson is Human Computer Interaction and she has more than 20 publications till now. The interviewee was an extremely valuable resource because of her experience with academic computer related issues.

Transcribed interview
In the start, we discuss about current mobile banking and then security issues related to mobile banking. She told us that security is a necessary for mobile banking because mostly people are hesitating to use mobile handset for transferring of lot of money. She told us that mobile banking is not user friendly but doing payment transaction through mobile banking is good idea and it is easy and every time customer can use it for bank services. We ask questions about authentication methods she told us that secure authentication method is a necessary for mobile banking. As bio metrics method is adopting in many departments for security purposes but in mobile banking it will be more effective. She told us that doing mobile banking through bio metric method finger print is more efficient. According to her bio metrics method (finger print) is more convenient and easy for authentication as compared to other authentication methods like voice, eyes etc. she told us that making bio metric authentication mechanism so that every customer can do mobile banking from any company mobile set.
According to her that customer is not adopting too much mobile banking as compare to internet banking so it will be a positive step introducing bio metrics method for mobile banking services. She told us that bank revenue will also generate more if more and more customer adopts mobile banking service. She told us that bio metrics method will ensure end to end security for mobile banking.
Transcribed Interviews
Interview 2

Name: Mats Henrikson
Email address: mats.henriksson@swedbank.se
Contact information: box 124,37222Ronneby
Dept. of: Management /IT
Company: Swedbank. Office Manager
Date: 07-06-2011
Start and End time: 10.00 – 10.45

The contacted person for interview was Mr. Mats Henrikson currently working as a office manager The interviewee was an extremely valuable resource because of his experience with management and customer related.

Transcribed interview
As we have discussed the current mobile authentication methods and how much customer keep trust. According to his point of view, there is a chance of exploitation the mobile banking authentication and due to this concern customer trust on mobile banking may affect. He told that if there is an extra authentication may improve trust and security in mobile. According to him the community of people always prefer where a new authentication method should be easy. A new account holder would be able to easy understand with the implementation of new authentication.

According to him, biometric is more preferable by all customers due to more convenient and popular in communities. And he believes strongly in future all device and system based on biometric because of security and familiar with easy use. He said if this biometric mechanism of authentication will help to improve the revenue of the bank and he said that new way of authentication is good to handle more customers in future without fear of authentication or security.

He suggested that finger print authentication method, if it implemented the trust will improve due to familiarity with secure method mechanism.

He told us that many customers are also doing banking on telephone but bio metrics method and especially finger print mechanism is more suitable as compared to any other mobile banking mechanism. He told us that easy and any time availability of mobile handset, it is more convenient and time consuming for the customer to do mobile banking which is an advantage for the customers as well as for the bank.
The contacted person for interview was Mr. Nisar Ahmad, currently working as an office manager. The interviewee was an extremely valuable resource because of his experience related to information technology of bank system.

Transcribed interview

First we discuss the current mobile authentication methods. He told us that mobile banking is convenient and easy method for the customers. The bank manager told us that customer is hesitating to transfer of huge amount of money using mobile handset. According to him, security plays a main role for customer satisfaction. He told us that end to end security insurance will help the customer to adopt more and more mobile banking. According to him, security level is increasing day by day for bank system and people appreciate when new and easy mechanism is presented to community.

He told us that now days many organizations are adopting bio metrics method so it is necessary to introduce bio metrics mechanism in bank sector because customer trust will be develop by adopting bio metrics mechanism. He told us that by finger print it will be surety for the bank that authorized person is using mobile banking.

He told us that there are many methods of banking system like telephonic banking, banking through mobile SMS but bio metrics banking is new mechanism and will be appreciable because it will minimize the doubt level of bank employees and improve customer satisfaction.

He told us that authentication of customer ensure us that authorized customer is doing mobile banking service. According to him, it is also necessary to ensure that customer data is secure at bank side. So in this way customer data will be fully secure from mobile handset to bank system and minimize the chances to hack the data.
Interview

Name: SumedhPaikrao  
Email address: sumedhpaikrao@gmail.com  
Contact information: oriental bank of commerce, Bombay, India  
Dept. of Information technology  
Company: oriental bank of commerce. Office Senior Manager · Jul 1993 to present  
Date: 12-07-2011  
Start and End time: 3.00- 3.37

The contacted person for interview was Mr.sumedhpaikrao, currently working as a senior office manager. The interviewee was an extremely valuable resource because of his experience related of information technology of bank system.

Transcribed interview

According to his view, current mobile handset authentication is safe for transaction. People also keen to get this type of service since it assures safe transaction for their need. He also emphasised that mobile banking does not have any impact in banking revenue but it will give better value added service for customers also in his point of view customer not giving grandness for more security for their regular transactions but business people awaiting for more authentication for end to end user.

When he talk about E-Commerce system, secure mobile banking enhance cooperate trust between buyer and seller likewise, he bring up some issues while customer facing with mobile banking likewise battery going down, Network availability and Virus attacks on mobile phone. He mentioned enhancement of E-commerce security issues that PIN based authorization, IMEINUMBER of mobile and mobile number to ensure authentication of the transaction.

He compared mobile banking with Internet banking, as per his perspective, customer more convenient with Mobile banking system when compared to Internet banking. He also emphasised that when the customer lose his mobile or his smart card they need to inform to customer service of the bank and immediately they will block their account to avoid further unauthorized transaction.
11 APPENDIX B

11.1 Questions for workshop

Q1: Do you prefer use of mobile banking for purchasing items or for bank services?
   A. Yes
   B. No
   C. Suggestion:_________________________________________

Circle your choice:
Q2: Do you think the proposed finger print scanner device in mobile banking services will increase the security level.
   A. Strongly Agree
   B. Agree
   C. Neutral
   D. Disagree
   E. Strongly Disagree
   F. Suggestion:_________________________________________

Q3: Customer satisfaction will be high by proposed finger print mechanism in mobile banking.
   A. Strongly Agree
   B. Agree
   C. Neutral
   D. Disagree
   E. Strongly Disagree
   F. Suggestion:_________________________________________

Q4: Fraud chances will be reduce by proposed finger print mechanism for mobile banking system.
   A. Strongly Agree
   B. Agree
   C. Neutral
   D. Disagree
   E. Strongly Disagree
   F. Suggestion:_________________________________________

Q5: The propose finger print mechanism is more suitable for authentication as compare to other bio metrics methods like voice, etc
   A. Strongly Agree
   B. Agree
   C. Neutral
   D. Disagree
   E. Strongly Disagree
   F. Suggestion:_________________________________________
Q6: Customer Trust can be developing by minimizing Fraud risk due to finger print mechanism?
   A. Strongly Agree
   B. Agree
   C. Neutral
   D. Disagree
   E. Strongly Disagree
   F. Suggestion:______________________________

Q7: Transaction of money will be safe by finger print mechanism and bank revenue will increase.
   A. Strongly Agree
   B. Agree
   C. Neutral
   D. Disagree
   E. Strongly Disagree
   F. Suggestion:______________________________

Q8: The proposed finger print mechanism for mobile banking is easy and accessible for bank services from anywhere.
   A. Strongly Agree
   B. Agree
   C. Neutral
   D. Disagree
   E. Strongly Disagree
   F. Suggestion:______________________________

Q9: The security level will be high by finger print mobile banking mechanism.
   A. Strongly Agree
   B. Agree
   C. Neutral
   D. Disagree
   E. Strongly Disagree
   F. Suggestion:______________________________

Q10: Risk level will be minimized by finger print scanner device? Authentication security level will be high?
    A. Strongly Agree
    B. Agree
    C. Neutral
    D. Disagree
    E. Strongly Disagree
    F. Suggestion:______________________________

Q11: Did Self-Efficiency will be increases by enrolling finger print mechanism in mobile banking?
    A. Strongly Agree
    B. Agree
    C. Neutral
    D. Disagree
    E. Strongly Disagree
Q12: Do you think customer will prefer finger print authentication mechanism as compare to SMS banking mechanism.
   A. Strongly Agree
   B. Agree
   C. Neutral
   D. Disagree
   E. Strongly Disagree
   F. Suggestion:______________________________