An Efficient Authentication Approach for Mobile Banking Users

Md. Javed Ahmed Shanto & Md. Zakir Hossain

A Thesis in the Partial Fulfillment of the Requirements

for the Award of Bachelor of Computer Science and Engineering (BCSE)

Department of Computer Science and Engineering
College of Engineering and Technology
IUBAT – International University of Business Agriculture and Technology

Fall 2020

An Efficient Authentication Approach for Mobile Banking Users

Md. Javed Ahmed Shanto & Md. Zakir Hossain

A Thesis in the Partial Fulfillment of the Requirements for the Award of Bachelor of Computer Science and Engineering (BCSE)

The thesis has been examined and approved,

_____

Prof. Dr. Utpal Kanti Das
Chairman

_____

Dr Hasibur Rashid Chayan
Coordinator, Associate Professor

_____

Prof. Dr. Abhijit Saha
Supervisor, Professor

Department of Computer Science and Engineering
College of Engineering and Technology
IUBAT – International University of Business Agriculture and Technology

Fall 2020

Abstract

Mobile banking is more easily and fast banking nowadays, but its challenges to payments security system. Many organizations or financial institution are now incorporating mobile and financial services as a key component of their growth strategy. We use bank to keep our money safe, but if we can't keep the money safe even in the bank where would we keep our money. Hence to keep our user's money to safe in a bank using digital system we propose to achieve greater efficiency using a new approach to use mobile banking system. We have proposed to increase the security of users to utmost level. Large number of security challenge of mobile banking payment system already have been proposed in the current research issues, but our goal is to take the mobile banking payment system more secure by using user's fingerprint. It will help to prevent hacking, phishing, sniffing or DoS attack. In our system we have proposed to use the user's individual fingerprint as we know that everyone has unique fingerprint. For securing our system more secure we will use128 bit MD5 hashing algorithm to generate auto hash code number that will be used by the user as an OTP. We are avoiding normal OTP that only generate 4-digit numeric value which is easy to hack. After that for every transaction we will use user fingerprint scan to confirm as it is also unique for everyone. We have researched many related papers and our system is unique than others. It's really important to increase the user side security. It will keep the hackers at bay. It's also easy to use because it's simple interactive and mostly efficient. We can implicate this work to any bank who offers E-banking services to their users, businessmen and govt. This proposed work is the future of user of banking security to feel safe to keep their money in the bank where there will be no chance of hacking and they can easily payment or withdraw their money at anytime

from anywhere. This work can be applicable to monetary services like International monetary Fund (IMF), visa card, master card, bkash and any other services available like those. A key challenge with gaining user adoption of mobile banking and payments is the customer's lack of confidence is security of the services. Understanding the mobile banking and payments market and ecosystem is critical in addressing the security challenges. Hence to conclude this proposed work will have great impact on the economic society and digital society of the future work of than bank and financial institutions.

Letter of Transmittal

19 December 2020
The Chair
Thesis Defense Committee
Department of Computer Science and Engineering
IUBAT–International University of Business Agriculture and Technology
4 Embankment Drive Road, Sector 10, Uttara Model Town
Dhaka 1230, Bangladesh

Subject: Letter of Transmittal.

Dear Sir,

With due respect sir, we are the students of 1710 batch who are trying to propose a thesis on "An Efficient Authentication Approach for Mobile Banking Users" under the networking sector of BCSE department. Though we in learning curve, this proposed work has enabled us to gain insight of network security and it's a wonderful experience. Without your inspiring, this report would have been an incomplete one.

We therefore, pray and hope that you would be kind enough to give us your judicious advice on our thesis.

Yours sincerely,

_____	_____
Md. Javed Ahmed Shanto	Md. Zakir Hossain
ID: 17103093	ID: 17103019

Student's Declaration

We declare that the work in this report titled "An Efficient Authentication Approach for Mobile Banking Users" has been carried out by both Md. Javed Ahmed Shanto and my partner Md. Zakir Hossain under the supervision of Dr. Abhijit Saha, Professor, Department of Computer Science and Engineering, International University of Business Agriculture and Technology. The information from this report has been duly acknowledged and no part of this report was previously presented or published to another institute or organization.

_____	_____
Md. Javed Ahmed Shanto	Md. Zakir Hossain
ID: 17103093	ID: 1710301

Supervisor's Certification

This thesis paper titled "An Efficient Authentication Approach for Mobile Banking Users" submitted by the group of Md. Javed Ahmed Shanto and Md. Zakir Hossain has been accepted as satisfactory in partial fulfillment of the requirement for the degree of Bachelor of Science in Computer Science and Engineering in December 2020.

_____

Prof. Dr. Abhijit Saha

Professor,

Department of Computer Science and Engineering

IUBAT–International University of Business Agriculture and Technology

Acknowledgments

We are really grateful because we managed to complete this thesis “An Efficient Authentication Approach for Mobile Banking User” (partly for now) within the given time. We can’t possibly think this proposed work without our advisor Prof. Dr. Abhijit Saha. He helped us to gain insightful information about networking security, algorithms and most importantly how to write a thesis paper in a detailed way. Thank you very much sir for your great advice. We also thank our chairman Prof. Dr. Utpal Kanti Das and our late chairman Prof. Dr. Md. Abdul Haque for their inspiration and last but not the least we would like to thank our Almighty and our family members for their constant support and secure of inspiration.

Table of Contents

Abstract iii

Letter of Transmittal v

Student's Declaration vi

Supervisor's Certification vii

Acknowledgments viii

List of Figures xi

List of Tables xii

Chapter I. Introduction 1

1.1 Background and Context 1

1.2 Current Methods and Evolution 2

1.3 Research Question 3

1.4 Proposed Work 4

Chapter II. Literature Review 6

2.1 Key Concepts, Theories and studies 6

2.2 Key Debates and Controversies 10

2.3 Gaps in Existing Knowledge 10

Chapter III. Research Methodology 12

3.1 Research Design 12

3.2 System Layout 13

3.3 System layout for Fingertips uses 14

3.4 Generating Hash Code as OTP 18

3.5 Methods and Sources 21

3.6 Practical Considerations 21

3.7 Testing.....22

3.8 Testing Methodologies:.....23

3.9 Front-End Design: 25

3.10 Home and Activities Front-End Design:.....26

Chapter IV. Result and Discussion.....29

4.1 Result and Discussion:.....29

Chapter V. Conclusion 32

5.1 Conclusion: 32

5.2 Future Work: 33

References.....34

List of Figures

Figure 3.1 System Layout 13

Figure 3.2 System Layout for Fingertips uses 14

Figure 3.3 Process of creating account fingerprint 15

Figure 3.4 Process of storing fingerprint data into server. 16

Figure 3.5 Simple view of Proposed System. 17

Figure 3.6 Generating Hash and sending to User 19

Figure 3.7 Checking Validation of Hash 20

Figure 3.8 User receive OTP 20

Figure 3.9 Front-End Design 25

Figure 3.10 Home and activities Front-End Design 26

..... 27

Figure 3.11 Database Design 27

Figure 4.1 Number of User Increasing in Mobile Banking 29

Figure 4.2 Other M-banking Vs Proposed M-banking 30

List of Tables

Table 3.1 Compatibility Testing 24

Table 4.1 M-banking App security on transaction..... 31

Chapter I. Introduction

1.1 Background and Context

Mobile banking is a service provided by a bank or other financial institution that allows its customers to conduct financial transactions remotely using a mobile device such as a smartphone or tablet. Mobile banking is utilizing terminal to perform those related banking transactions. It combines the currency electrification and mobility to offer new kind of banking service and allows people can perform a lot of different kind of banking service in any time at anywhere. As adopting M-banking, there are some advantages listed in the following (Hanacek & Malinka, 2010).

I. No Restriction of locations: The user can perform banking anytime in any place as possible

II. Personalization: Each of the mobile phones is dedicated to a specified user. Therefore, it increases the effectiveness of user authentication.

III. High Penetration: The popular utilization of mobile phones provides the sufficient assurance of the growth and utilization of M-banking.

A mobile banking is when banks offer their services to the customer through mobile phone. Earliest mobile banking started from 1999 in Europe through WAP enable mobile phone. They offered their services by SMS then. It was known as SMS banking too. Before 2010 maximum mobile banking performed by SMS or mobile web. After 2010 all of the bank started to change their approach to mobile banking as the news of hacking was increasing day by day. There are several types of mobile banking system. For example, mobile banking through mobile applications (mainly through smartphones and internet), mobile banking over

SMS which is also known as SMS banking and mobile banking over unstructured supplementary service data (USSD).

Hence the question remains. What is the major threat or risk of mobile banking? There are several. Mobile Malware, Poor App design, configuration or corrupt apps, lost or stolen devices, unsecured Wi-Fi networks, identity theft, mobile device ID vulnerabilities, remote deposit capture fraud, social engineering and hence on. Hence how can we get rid of these vulnerabilities? How can we safely transect through mobile banking? The answer is simple actually. Research more on mobile security, increase firewall security, keep an eye on every doubtful transaction, increase fault tolerance, secure the TCP/IP model etc. Our proposed work is one of them (Zhuang, 2012).

Mobile banking is one developing high dynamic technology which is used in the commercial areas. It has combined two applications: one is information technology and second is commerce applications together. Since Mobile banking was introduced, customers have been able to use it to obtain all mobile banking services whole day without having to visit the traditional bank branch for personal transactions. But there are various types of attacks that M-banking can suffer. They include Social Engineering, Port Scanners, Packet Sniffers, Password Cracking, Trojans, Denial of Service Attacks, Server Bugs, and Super User Exploits (Omariba & Masese, 2012).

1.2 Current Methods and Evolution

There are several current methods to improve mobile banking. In them the most effective are multi-factor authentication system, using NFC embedded SIM card, end to end encryption, real time text and emails alerts, block-chain’s work is increasing and its good, utilizing behavior analysis, safe digitized access, protecting session information, digitized user

identification, preventing cross channel infection and last but not least increasing the security of firewall. The current methods are effective in many aspects of the security. But hacking is increasing with the speed of light too. Using social engineering hacking is increasing, digitized id is hack-able too using DOS or other hacking methods. Multiple authentication system is also can be hacked nowadays. We can replace the original SIM with a fake one and get the OTP banks are sending. NFC SIM can be stolen; we can block through flood attack the real time text and emails. All though block chain is better and a safe guard for mobile banking, it's costly and can't be used by a huge audience. Nowadays the data server is targeted mostly as the hacker can get any information of any user. And it's terrifying. Using SQL injection, it can be done.

Hence to prevent that a better secure system for mobile banking is only time demanding.

1.3 Research Question

a. What would be the future of mobile banking in our country?

b. How we can use our latest technology in mobile banking and increase the security at its utmost.

c. What is the limitation of present mobile banking system and why will be our new system better than any other system?

d. In which sector can we implement this system?

e. Is the system can be used by everyone?

1.4 Proposed Work

As we have seen how the mobile banking is targeted by the hackers frequently, we need to prepare a better secure, easy to use or simple app. We have researched a lot of research paper for mobile banking. As far as we have seen the best technology is now using fingerprint as password for mobile banking. But as we know it is not well-versed way or its not used by every bank. The recent Bangladesh bank reserve theft has a good impact on our thought how can we deal with this kind of hacking or stealing. That's why we thought the importance of a secure banking security and we approached this method. It's a secure app which ensure the security when a user enters the app and as well as in the time of transaction.

We aim to develop this project to utmost level what we can. It can be used in any banking organization, monetary sector, even we can implement this in government project also. We aim to research it further to implement this in a real-life sector. In the area of mobile banking security hence many securities system is already available nowadays. But even after that almost every day there is something happening to someone that is related to mobile banking security. For that we are trying to make a system that will be simple but more secure than any other system. Our contribution will be a system design that will be able to take user bio-metric for making transaction which will make the system simpler but secure. This system will be relevant to all the mobile user who basically use mobile banking system for their daily life. It will create new opportunities to use bio-metric system in mobile banking app by the general public. It's worth doing because it will change the opinion of security system of mobile banking security. Our system covers almost everything with the fingerprint as password, 128-bit automatic generated hash code instead of OTP (one time password). And for every time a user wants to do a transaction, send money, cash out, transfer money, or even payment for

something user needs only fingerprint scan through their own smartphone. We think it will be most secure system for mobile banking the world has ever seen.

Chapter II. Literature Review

'Mobile banking and economic development' for over a decade, the rapid development in information and communication technology has significantly affected the banking industry. Mostly the financial sectors and the banking sector have improved their services through implementing various information technologies. From all of them mobile phone is one of the most recognized and well accepted technologies not only in the developed countries but also in Bangladesh. But recently in Bangladesh it is observed that traditional branch banking is going to reduce due to increase in mobile banking where weber started that the use of mobile phones nowadays in order to effectuate banking transactions in bound to increase in a significant way in near future. According to Donner, Jonathan, Tellez, and Camilo ―the terms mobile banking, m-payments, m-transfers, and m-finance refer collectively to a set of applications that enable people to use their mobile telephones to manipulate their bank accounts, store value in an account linked to their handsets, transfer funds, or even access credit or insurance products (Donner & Jonathan, 2008).

2.1 Key Concepts, Theories and studies

"A review on advanced security solution in mobile banking models". In their research they tried to build a system instead of WWW or WAP. In early days the E-banking system mostly depend of the WWW which has to relay on some specific devices and those devices are not easy to carry everywhere. To come out form that situation they found and build a system which is not relay on WWW or WAP and most importantly they wanted to focus on Personal Network Provider system to include in their build system. But at this digital era of time only depending on only Personal Network System Provider is not a good thing. Hackers can get

into their system easily. For those reason here in their research they are moving from the internet banking to Mobile banking for more security. To enhance the security for the online financial transaction, a biometric fingerprint authentication system is also proposed by them. In their paper, the feasibility and limitations of an advanced biometric fingerprint authentication system for mobile banking system are discussed. Mobile as we all know that is a personal device, usually with a built-in display and keyboard, are well-positioned to provide a technical solution for reducing fraud and allowing the fair allocation of responsibility for damages from fraud. As mobile phone is also a secure device nowadays some amount of security is already part of the authentication mechanism of existing mobile phones as a way to prevent call theft. They also provide some secure transactions process using mobile phones (Aithal, 2016).

1. Identification Process: In this process the device identifies the user or customers through physical possession as with regular mobile phone it is capable of having or generating biometrics or face recognition process.
2. Authentication Process: Here the process is that the mobile banking services provider authenticates the transaction request from the device via either subscriber identification which is available with the existing phones or cryptographic mechanisms such as digital signatures or secure protocols like Wireless Transport layer security Specification.
3. Secure Performance: In this performance process the financial transaction is performed by the mobile banking service provider, possibly with the help of the merchant and the other transactions providers for bill payments and may involve secure payment protocols.

4. Confirmation: When all the process will be done for payment or transferring a confirmation of the completed transactions is deliver to the user.

"Secure OTP and Biometric Verification Scheme for Mobile Banking" In this research paper they made a system which has the facility of OTP (One Time Password) and biometric for confirming the security of mobile banking payment system. In order to rise the security of M-banking, some banks adopt the one-time password (OTP) to remedy the possible M-banking stealing risk. In the past OTP is sent to personal mobile phone. But currently most of the smart mobile p hone can performing M-banking easily. Thus, it gains higher risk of information security due to mobile phone hacking. In order to provide a reliable and secure M-banking process without risk they have combined the personal biometric system with the OTP. The server side will generate an OTP and send it to the user for a limited period of time. Then the user will use that OTP and the server side will check its validation. After that the server side will send a request to user to capture personal biometric for further verification. Their proposed scheme not only provide secure M-banking but also can clearly define all the process (Deng, 2012).

"Intelligent Quality Performance Assessment for E-Banking Security using Fuzzy Logic" In their research they have found security has been widely recognized as one of the main obstacles to adoption of Internet baking. They have proposed that Using Fuzzy logic (FL) Model can be an effective model tool in evaluating of e-banking security performance and quality. Their proposed model was based on FL operators and produces four measures of security risk attack dimensions which is direct internal attack, communication tampering attach, code programming attack, and denial of service attack with a hierarchical ring layer structure. And

they have found form their research that direct internal attack risk has a large impact on e-banking security performance. The result also confirms that the risk of direct internal attack for e-banking dynamic websites is double that of all other attacks

“Mobile Banking Transaction Using Fingerprint Authentication “Now a days password based protection system is everywhere and it’s the most approaches way to protect any systems. But there are many problems associated with the password based authentication systems and the risks associated with using passwords as an authentication mechanism for enterprise applications is not completely secure. For password bases protections systems one of the most common problem is most of the users forget their own password. Along with that they have discussed few downside to password based system of password based mobile banking systems those are:

a) Security vs. Ease-of-Use for Passwords
b) Single high-value target
c) Does not provide strong identity
d) Weak and susceptible to numerous attacks.
e) Shoulder Surfing Attack

To prevent this types of vulnerability they come up To reduce the potential vulnerabilities regarding to the security, a combination of user id & password and fingerprint recognition system seem to be one of the most reliable means of authentication in a, mobile banking application environment. (Mathuria, 2018)

2.2 Key Debates and Controversies

In those papers they have tried to secure the e-banking and mobile banking more secure in different way where our proposed system will be also different from their work. They have used some algorithm to check and secure the risk of hacking in e-banking system in internet. And for mobile banking system differently they have used OTP and biometrics for making the system more secure. But In this time we know that an OTP is only 4 digit numeric value which can be easily hack by the hacker using brute force attack. But what we are proposing is instead of OTP we are using the MD5 hash algorithm to generate auto hash code which will be used as OTP. We are replacing OTP to Hash and the reason is that hash is almost impossible to hack. And they use only biometric to their system and we will implement a system that will require biometrics for confirmation the transaction process.

2.3 Gaps in Existing Knowledge

Those research paper shows that no one is using the both system OTP and Biometrics at a time. If they could do that their work could have been better than what they have done. Among them one only using the private network for securing the system and others are using only the OTP for making the system more secure. But our proposed work will fit in this those research paper shows that no one is using the both system OTP and Biometrics at a time. If they could do that their work could have been better than what they have done. Among them one only using the private network for securing the system and others are using only the OTP for making the system more secure. But our proposed work will fit in this because in our work I'll be using the MD5 Hash algorithm to generate 128bit unique code instead of OTP which is

more secure than the actual OTP system and along with that in our work we'll use user fingerprint for making the system more secure.

Chapter III. Research Methodology

3.1 Research Design

Our implemented system will be always connected to the bank server Hence that it can it's all kind of transaction in short time and easily. For using the system, a user must need to register or have a bank account. System will take user's fingerprint for the security purpose and store those data to the bank database. And only after those process a user can use the system. For using the system, a user first need to put his account number after that they can request for a hash code or he can use biometric. After that he can access his account and can do some other tasks but only for making transaction, he need to fingerprint scan for more security purpose and that is out main research.

3.2 System Layout

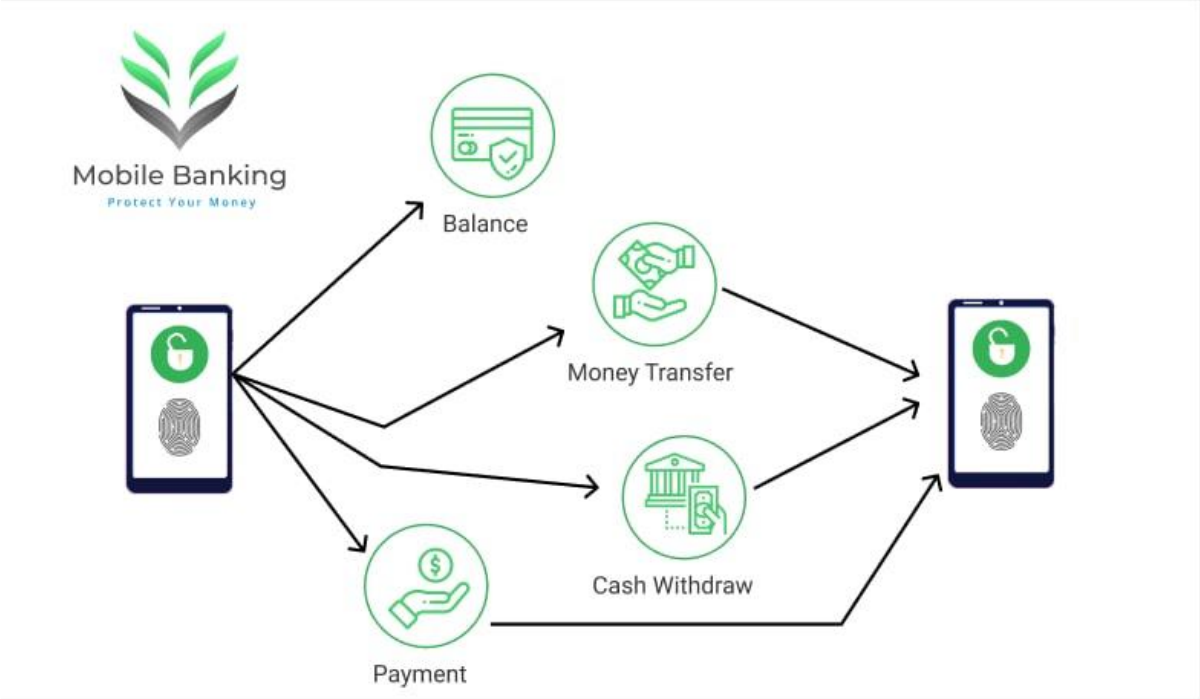

Figure 3.1 System Layout

The figure 3.1 is shows that Mobile Banking gives users instant connectivity to their accounts anytime, anywhere using the banking apps on their mobile device, allowing users to access account details, history and check account balances, which increase convenience for the consumer, while reducing banking costs. Here what we are seeing the system layout of the mobile banking system. First user needs to login to their own bank account using our own generated system approach which is using fingerprint or by requesting the Hash to use as OTP (One Time Password). After login to the account, they can access the features of the bank here we are showing only the common and necessary features that a user needs nowadays. For example, checking the balance of his account, cash withdraw, payment and money transfer.

3.3 System layout for Fingertips uses

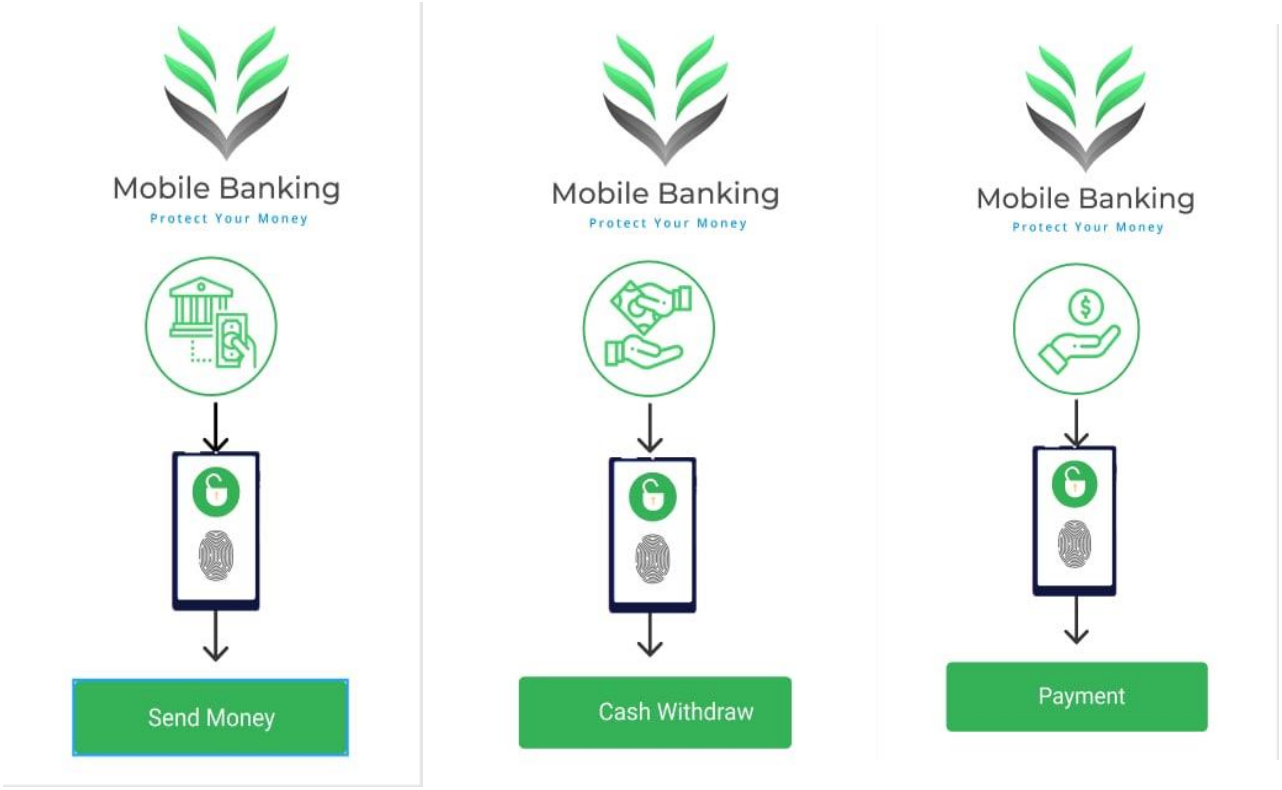

Figure 3.2 System Layout for Fingertips uses

In figure 3.2 it's showing that after login to the account user will see the features of money transfer, payment, and cash withdraw. If the user wants to transfer money to any other user's account or if the user wants to payment for anything or if wants to withdraw money in that case the user will need to scan his/her fingerprint for making all those things happen. And scanning finger will take very less amount of time and will be a 100% secure system for the user.

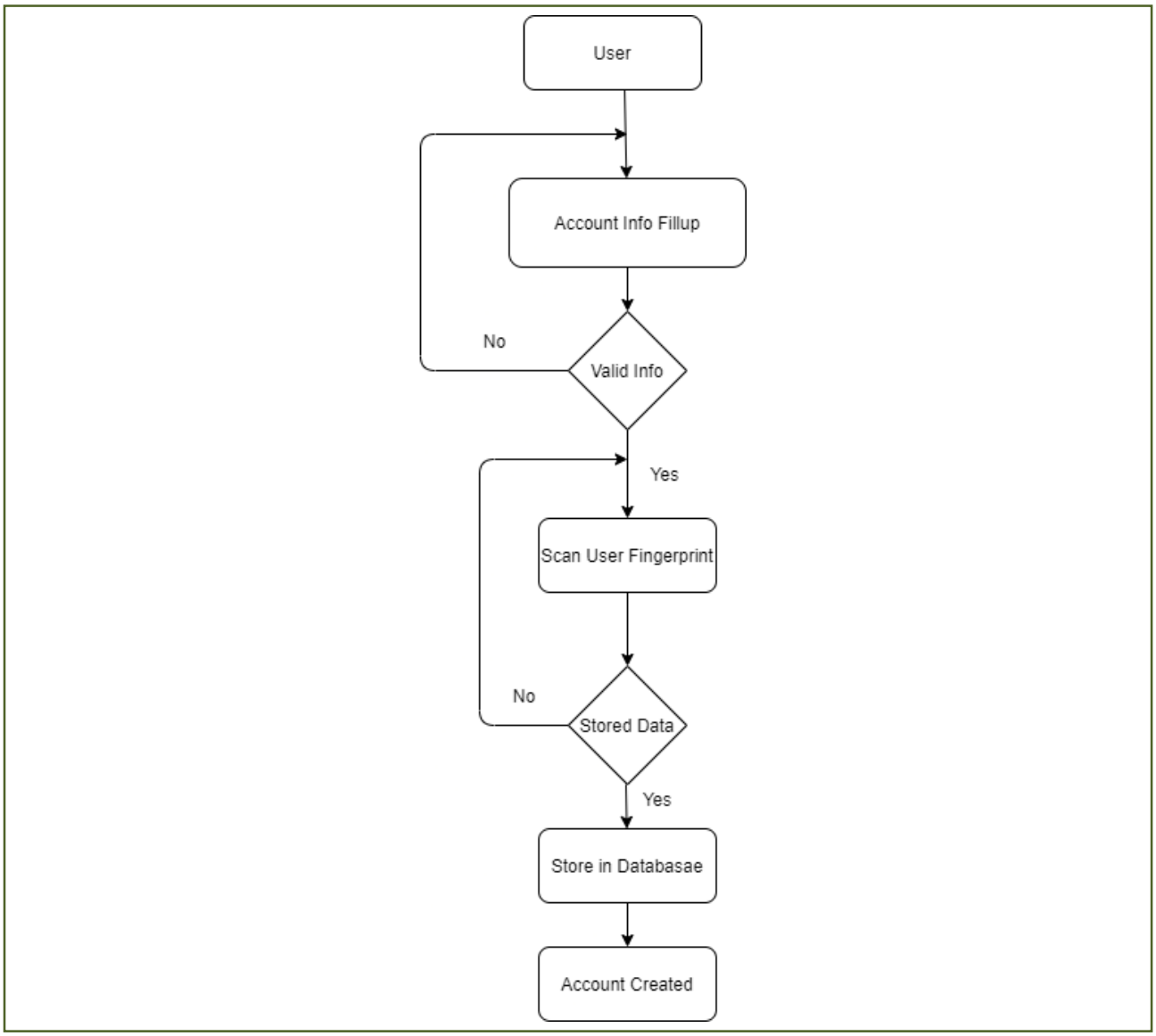

Figure 3.3 Process of creating account fingerprint

Here in figure 3.3, we can see the process is.at first a user needs to create an account to use the bank services. First of all the user need to provide all the valid information of his or her who want to create an account. After giving all those information from the bank they will provide scanner to scan user's fingerprint. After taking those things those data will store into the bank server. After storing the data into the bank server successfully the account will be open for the user.

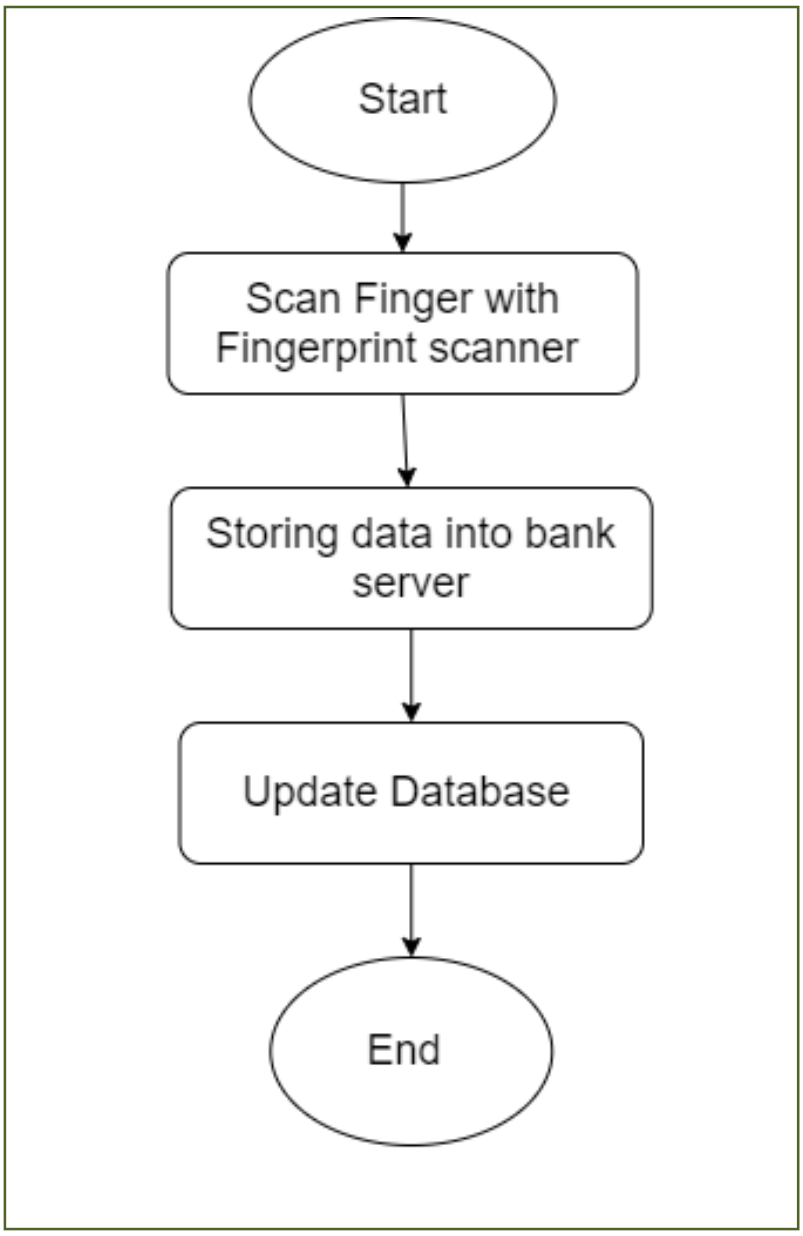

Figure 3.4 Process of storing fingerprint data into server.

Figure 3.4 shows that in this process here the data will be stored into the bank server. After scanning the user fingerprint from the device, the data will be sent to the bank server. If bank server can successfully store the data, then it attaches the given information and account of the bank with those data of fingerprint.

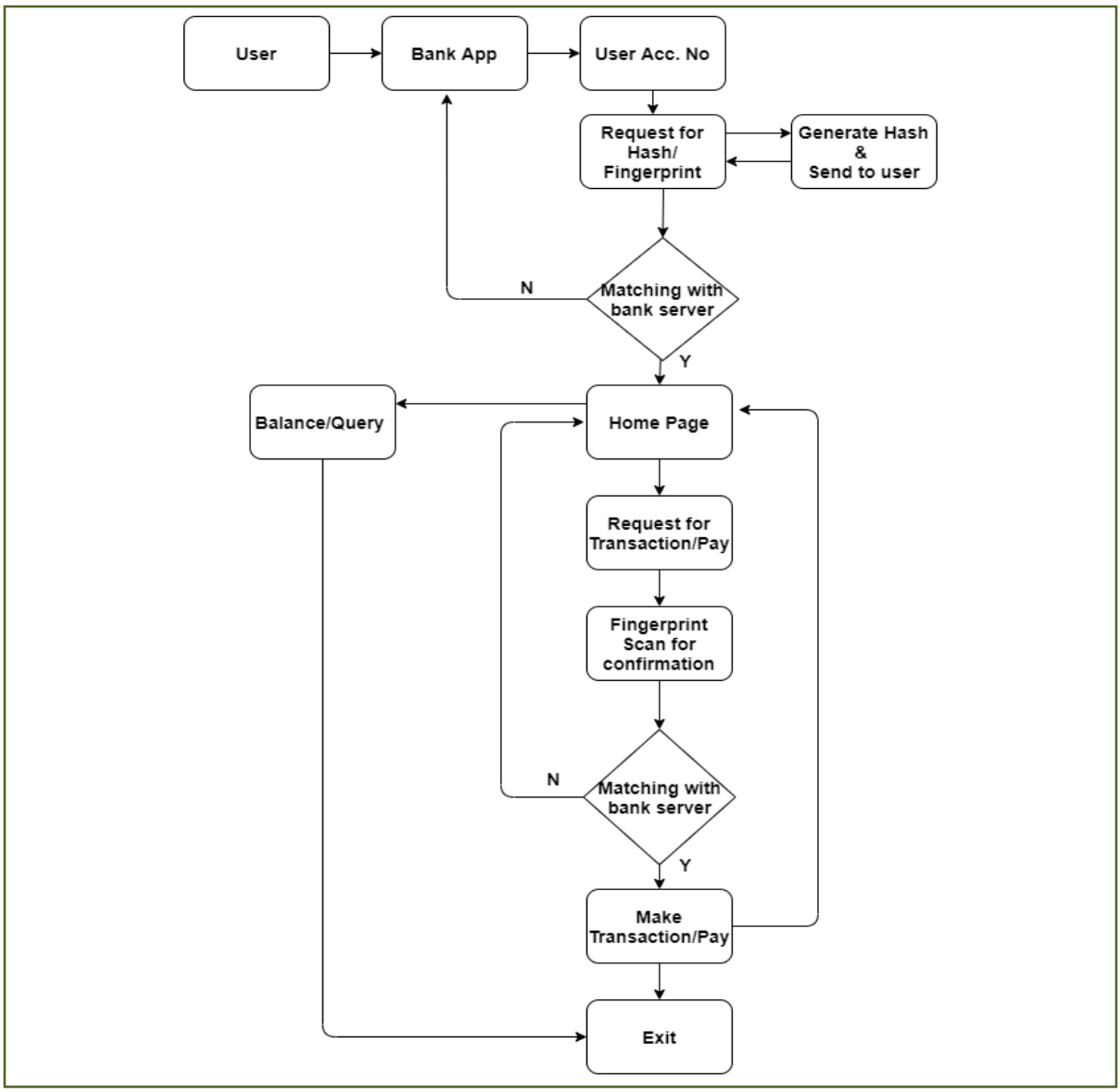

Figure 3.5 Simple view of Proposed System.

Figure 3.5 shows the full proposed system model. The work here is very simple but secure at the same time. First of all, user will open the mobile application that is provided by the bank using our security system. After opening the application user need to insert their bank account number. Then after giving the bank account number user will see option if they want to login to their account with using fingerprint or want to use OTP which is actually 128bit hash code. If the use chooses to use fingerprint, then they can use their mobile's fingerprint to scan their

finger and after scanning the data will receive by the bank server and bank server will try to match the predefine data with this new data if it matches only then the user can see the home page or default page of their account from the app. If anyone want to use the Hash, they will need to send request to the bank server and from the bank server a unique hash code will be send to them and they will use that code and the bank server again check if they put the valid hash or not if it matches then they can see their home page of their account. After that if they want to make payment to anyone or want to withdraw money in that time, they will be asked to scan their fingerprint each and every time they are going for payment of transaction. This process will be taken every time they want to make payment or transaction. This will give the system an extra layer of security.

3.4 Generating Hash Code as OTP

As we are trying to remove the use of OTP and want to use hash code instead of OTP by the help of MD5 hashing algorithm. Though there are lots of hashing algorithm among them SHA1 is also famous but the reason for using MD5 algorithm to generate hash code is the speed. The speed of MD5 is fast in comparison of SHA1's speed and it is simple than SHA1 algorithm.

Here is the sample python3 code for generate MD5 hash and send the hash as OTP for user and also checking the validation of the hash. For sending the OTP in mobile phone we need the API access. For free API we use the Twilio. By using this Twilio we are getting the authentication key and id with a phone number. We are using those for testing purpose.

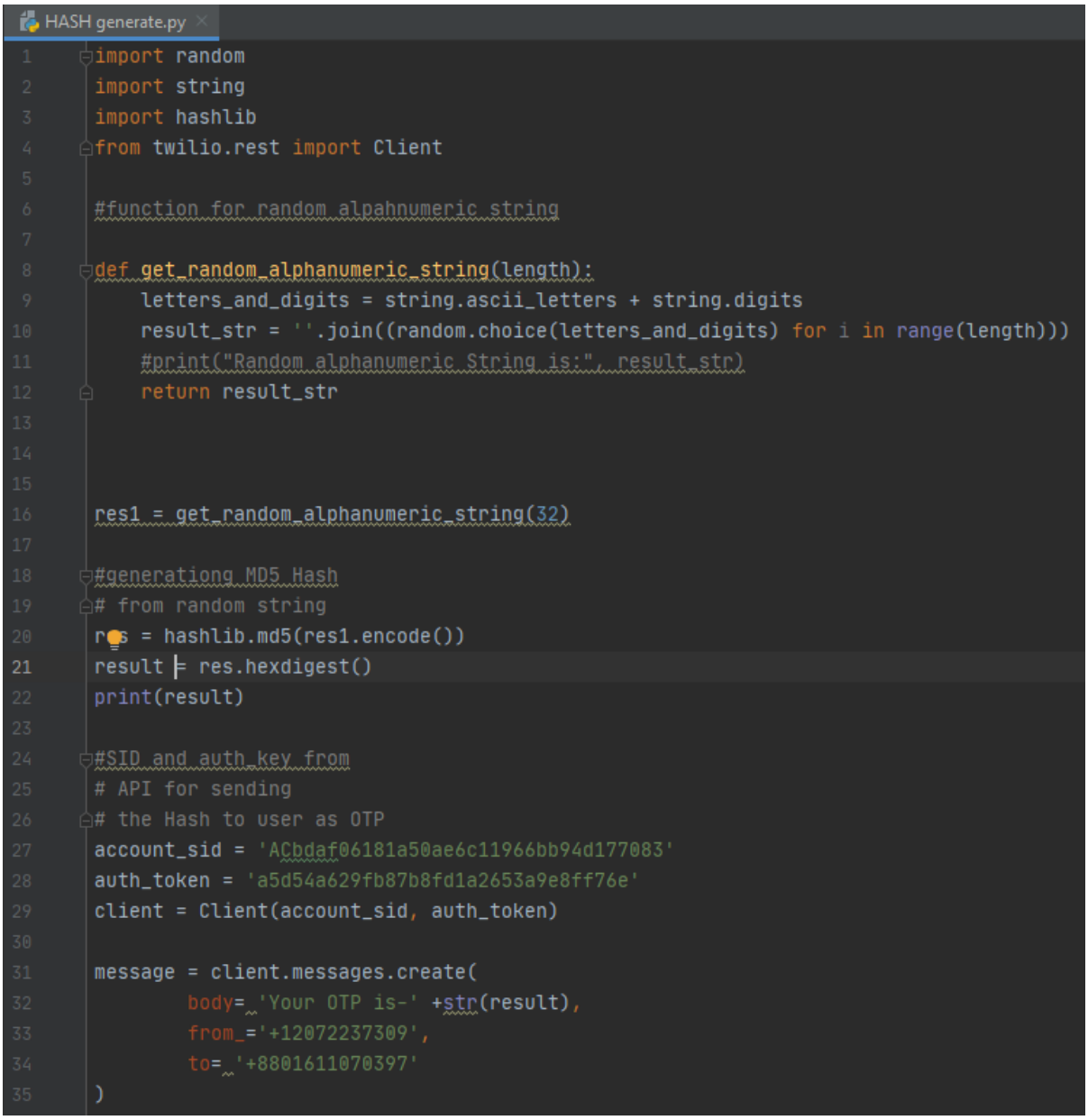

Figure 3.6 Generating Hash and sending to User

Figure 3.6 shows the process of generating Hash code in python and sending it to the user using user's phone number. By this process of the system, we can ensure that each time users trying for login to their mobile banking account is getting unique hash code as OTP.

```
36
37
38  #Checking the validaion of Hash
39  print(message.sid)
40  v = input("Enter Your Hash")
41  if v == result:
42      print("Successfully login with Valid Hash")
43  else:
44      print("Hash is not valid!!! Please try again ")
```

Figure 3.7 Checking Validation of Hash

Figure 3.7 shows the process of validating the hash code from user. In the time when user will put the hash code they got into their mobile phone from the system and they put the hash code to the system that the user's hash code is matching with the system's generated hash or not.

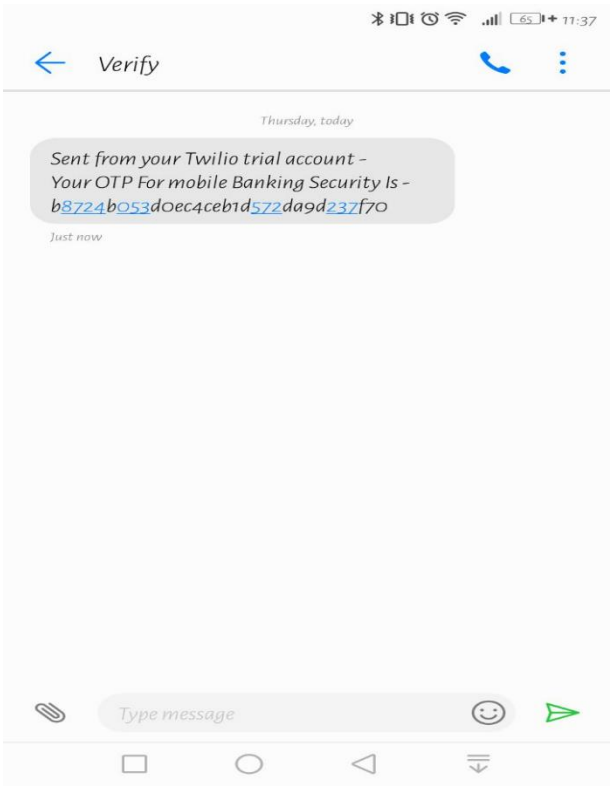

Figure 3.8 User receive OTP

In figure 3.8 shows that user get hash as otp/hash code in their mobile phone. The user must use the same hash code to verify their login to the mobile banking system.

3.5 Methods and Sources

Mobile Security Framework is an automated mobile app security testing tool for Android and iOS apps that is capable of performing static, dynamic analysis and web API testing.

For designing the prototype of our proposed system, we use “Figma”. Figma is a vector graphics editor and prototyping and code generator tool which help in primarily web-based, with different offline features enabled by desktop applications. The Figma is mirror companion apps for Android and iOS allow viewing Figma prototypes on mobile device. We use Figma to show how our proposed system for mobile banking security system will work for the user. For login to the system, they can use their fingerprint to access the home page or they can make request for the Hash code to access the home page. After that they will be able to do banking related task like as payment, cash withdraw, send money those kinds of activities. For making those things happen user need to scan their fingerprint each and every time. This will take only few seconds to do.

3.6 Practical Considerations

For using the system user must need a mobile phone which will be used for the process of fingerprint scan. But all the mobile phone doesn’t have the facility of this. For this a user must need to a phone that can scan fingerprint but that will cost a lot. Hence not everyone will be able to use the system in a particular way. At first time we need to do marketing for making

people understand the value of this system otherwise people will not show any interest in this new technology or new system

3.7 Testing

This project was judged on the following set of criteria

Satisfying Requirements Specifications: The project is successful it satisfies all the all the requirements, such as functional and non-functional requirements. In other words, it should be capable of ensuring the requirements specifications.

Correctness: It is one of the critical requirements of software development. Perfectness is the primary demand for service-oriented software. Every part of the application should work correctly and accurately.

Compatibility and Integrity: These are some necessary conditions to check whether or not the program is successful. This mobile banking system is created to be compatible with any domain. It was also designed in such a way that it could persuade the virtualization depended on how the application was implemented to the whole system.

Real-time management: The application is about which puts the power to save a life in the palm of people's hands. Hence, it is necessary to maintain a scenario. The users of this system should have the ability to maintain this.

Reliability and security management: Security is one of the crucial factors in any service-oriented systems. Thus, the evaluating criteria on the security features had been taken into account when the system was developed.

User-friendliness: Friendliness in any application is also a particular criterion to judge the systems. For instance, the users of this solution should feel contented when they are using the system. In essence, a system should have quality measures properties, such as efficiency, portability, reusability, flexibility, cohesion, and loose coupling among different components of the designed software.

3.8 Testing Methodologies:

Software Testing Methodology is defined as strategies and testing types used to certify that the Application under Test meets client expectations. Test Methodologies include functional and non-functional testing. Examples of Testing Methodologies are Unit Testing, Integration Testing, System Testing, Performance Testing, etc. Each testing methodology has a defined test objective, test strategy, and deliverables.

Functional Testing: Functional testing involves testing the application against business requirements. It incorporates all test types designed to guarantee each part of a piece of software behaves as expected by using the design team or business analysts use cases. These testing methods are usually conducted in order and include:

- Unit Testing
- Integration Testing
- System Testing
- Acceptance Testing

Non-functional Testing: Non-functional testing methods incorporate all test types focused on a piece of software's operational aspects. These include:

- Performance Testing
- Security Testing
- Usability Testing
- Compatibility Testing

Unit Testing: Unit testing is the first level of testing and is often performed by developers. It is the process of ensuring individual components of a piece of software at the code level are functional and work as they were designed. The rationale of the unit test was to find out the defects in this Project.

Compatibility Testing: Compatibility Testing, part of software non-functional tests, is tested to evaluate the computing environment's application. software compatibility testing can be more appropriately referred to as a user experience environment.

This Project is tested on different types of android mobile to ensure the following.

Table 3.1 Compatibility Testing

Android Device Name	Screen Size	Test	Result
Xiaomi Redmi A2 Lite	5.84 inch	Yes	OK
Huawei GR5	5.5 inch	Yes	OK
Walton Primo GM3	5.34 inch	Yes	OK
Samsung Galaxy A5	5.00 inch	Yes	OK
Samsung Galaxy A3	4.5 inch	Yes	OK

3.9 Front-End Design:

The screenshots below show the main system view. Capture and image of what you'll see on your mobile screen.

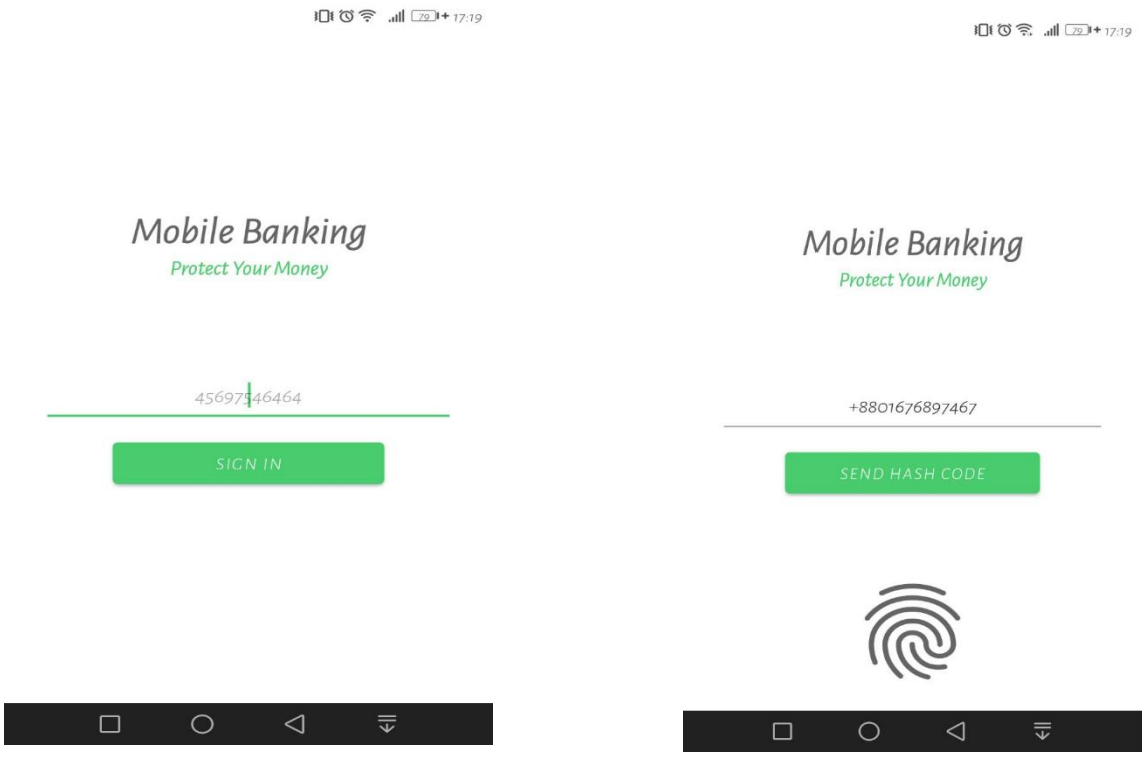

Figure 3.9 Front-End Design

Figure 3.9 shows that we can give our Account no here. And after that we can directly go to the home page of the app. If we can't get into the app for some reason, we can give our phone no and request the otp or hash code.

3.10 Home and Activities Front-End Design:

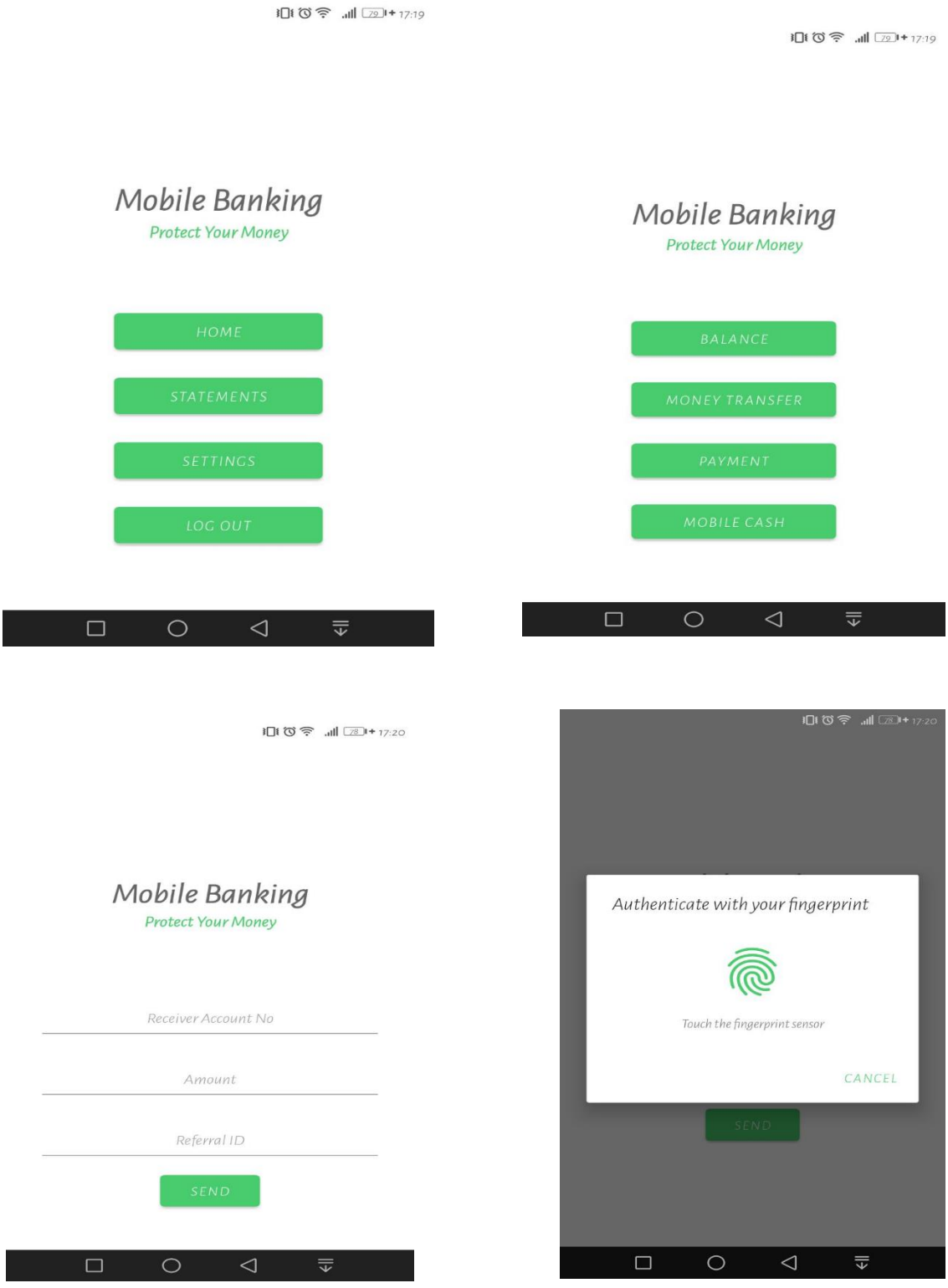

Figure 3.10 Home and activities Front-End Design

Figure 3.10 shows the home app design where we can roam around and go for the action what we want like checking balance, transferring money, payment etc. and for every transection we will need the fingertips and we will match it with our bank database. If it matches than we will give him/her permission to proceed transection.

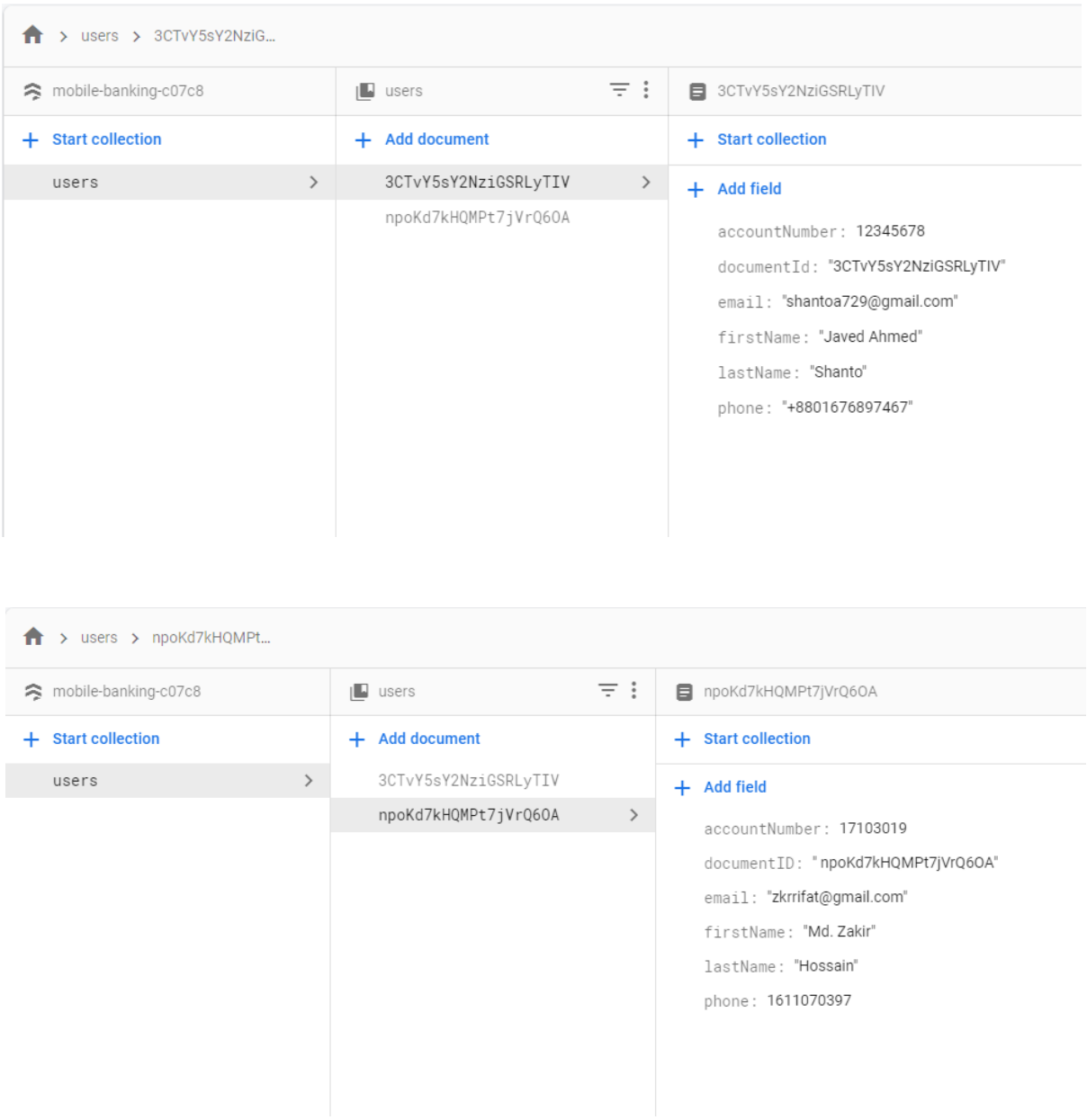

Figure 3.11 Database Design

Figure 3.11 shows that user records and user details of individual from the database

Chapter IV. Result and Discussion

4.1 Result and Discussion:

An authentication model is proposed thorough design process. The system design was validated by conducting a workshop. The analysis of the workshop's results showed that the bank customer's trust in security for mobile banking will be increased by our system security design. To promote mobile banking, it is necessary to improve customer trust in terms of security.

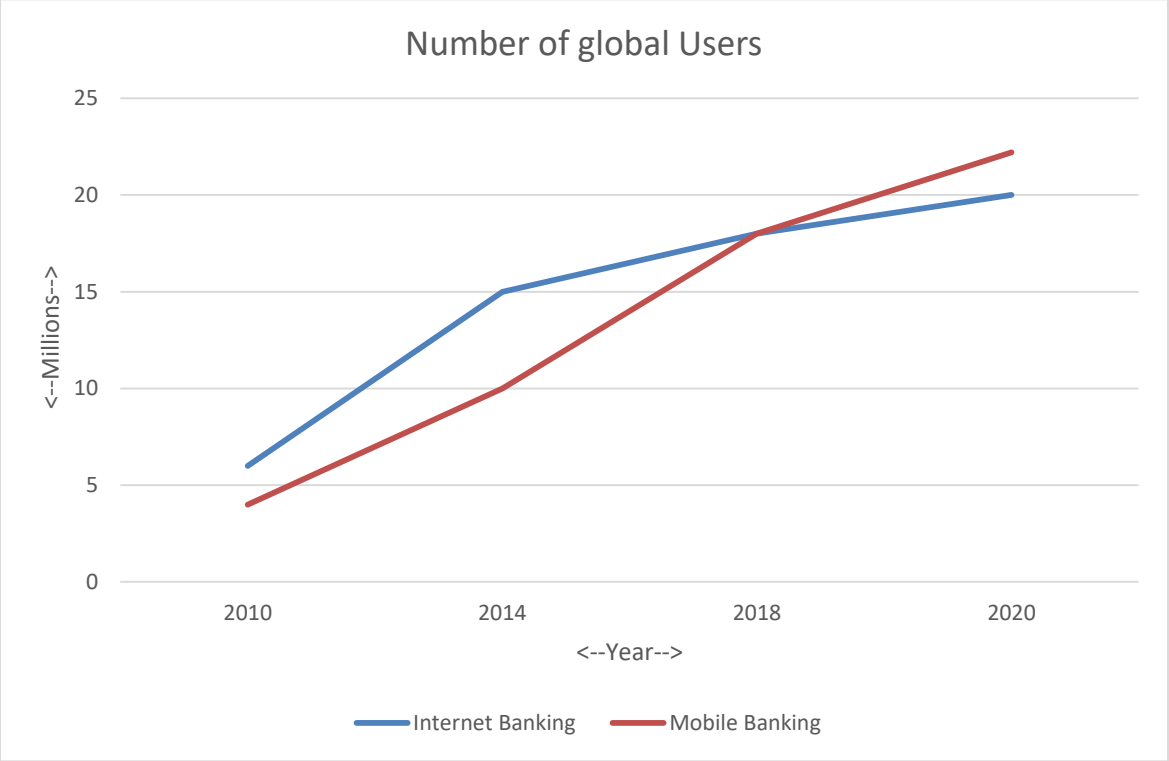

Figure 4.1 Number of User Increasing in Mobile Banking

From figure 4.1 we can understand that the user of mobile banking is increasing day by day in a big amount. For increasing the number of users, it is becoming more vulnerable for the hacker. For this the system of mobile banking must need to be more secure. To make the system more secure we have come to this fingerprint security system for the mobile banking system.

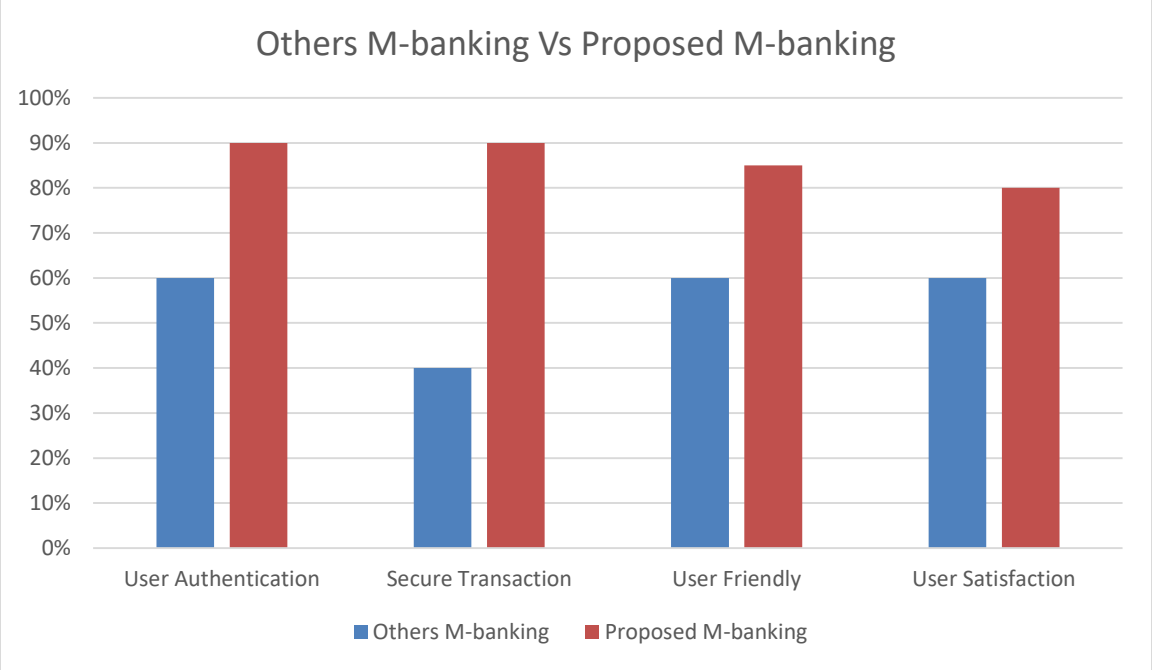

Figure 4.2 Other M-banking Vs Proposed M-banking

From figure 4.2 we can see that normal mobile banking nowadays are basically using the OTP and password system and those passwords are mostly numeric value for most of the mobile banking system which is easily breakable by the hacker. Instead of those easy vulnerable numeric passwords if we use the system, we are trying to build will be more secure. We can see that for user authentication for the normal OTP is less workable than the fingerprint bases mobile banking system. And most importantly which is require nowadays is secure transaction

system. Fingerprint based transaction system is more secure than the OTP based system and more user friendly.

Table 4.1 M-banking App security on transaction

M-banking App	Passcode	OTP	Fingertip	Secure
Rocket	Required	Not available	Not available	70%
Bkash	Required	Not available	Not available	65%
Nagad	Required	Not available	Not available	70%
AB bank	Required	Available	Not Available	80%
National Bank Ltd.	Required	Available	Not Available	80%
Proposed M-banking	Not required	Available	Available	90%

Table 4.1 shows that our conventional methods of existing online payment system vs our proposed system and their security percentage.

Chapter V. Conclusion

5.1 Conclusion:

Mobile banking rapidly increases to make easy payment system, user can access any time baking to make any payment. Attacker always makes a new program to attacks our mobile and get personal information. Hence, organizations and mobile banking user must work together with operating system and network provider Company that make a most reliable and user trust security system. The mobile banking payments system nowadays is more challenging and dynamic. It is changing rapidly. Mobile banking can provide services which transcending above the limitation of time and space. In the system we mainly focus to do three things

1. Storing the currency in an account accessible via the handset with proper security within it. When the user will have the bank account and use the system in their mobile phone, they will get the full service from the system.
2. Convert cash in and out of the stored value account without thinking of the security for sending the money by mistake. In the most flexible services, a customer can visit a corner kiosk or grocery store to give his payment without any hassle with full security each and every time.

3. Transfer stored value between accounts. Customer can easily generally transfer funds between accounts which is also highly secure.

In this thesis, we introduce and validated design method for mobile banking by using bio metrics 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 form professionals and bank experts.

In the first step, it was observed that there is lagging of security and there is no formal authentication between the customer and the bank in the meantime of making transaction and making payment. Hackers can easily cyberpunk and there is no assurance the bank authenticates the authorized person. For this reason, authentication in time of making transaction is introduced to improve the mobile banking security.

In the second step the method based on designing is define by using both strengths and weaknesses of current authentication mechanism.

This thesis fulfills the gap of authentication between the customer and the bank. From here we can see that the system increases the security level between the user and bank. The security will also increase the bank revenue.

5.2 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 and also for user identifications. As a future plan it has been planned to replace the fingerprint with retina scanning for the payment and the transaction process. If this is possible to implement this ensures secure authentication thereby increasing the bank revenue and reducing the networking problems which arise mainly due to congestion and unauthenticated session.

References

Aithal, S. (2016) ‘A Review on Advanced Security solutions in online Banking Models’. Srinivas Institute of Management Studies, India.

Avdic, A. (2019) ‘Use of Biometrics in Mobile Banking Security Case Study of Croatian Banks’, International Journal of Computer Science and Network Security.

Bilal, M. and Sankar, G (2011) ‘Trust & security issues in Mobile banking and its effect on Customers’ School of Computing, Blekinge Institute of Technology

Donner and Jonathan (2008) ‘Mobile banking and economic development’. Asian Journal of Communication.

Deng, J. (2012) “Secure OTP and Biometric Verification Scheme for Mobile Banking”. Institute of Digital Mechatronic Technology, Chinese Culture University.

Hanacek, P and Malinka, K. (2010) “e-Banking Security-A Comparative Study″. IEEE Aerospace and Electronic Systems Magazine.

Kelvin, C and Ming, k. (2008) “Security of Mobile Banking”. University of Cape Town, South Africa.

Mathuria, M and Sharma, L, (2018), ‘Mobile Banking Transaction Using Fingerprint Authentication’, International Conference on Inventive Systems and Control

Omariba, B. and Masese, B. (2012) “Security and Privacy of Electronic Banking”. International Journal of Computer Science.

Steiner, B. (2015) “E-banking security and organizational changes”. University of Liverpool.