A framework of biometric recognition and personalized mobile application to establish a dynamic connection with the ATM to enable secure transaction.

By

Syeda Prima Tasnim
16366008

A thesis project submitted to the Department of Computer Science & Engineering in partial fulfillment of the requirements for the degree of
M.Engg in Computer Science & Engineering

Department of Computer Science & Engineering
Brac University
August, 2019

Declaration

It is hereby declared that

1. The thesis project submitted is my/our own original work while completing degree at Brac University.
2. The thesis project does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. I/We have acknowledged all main sources of help.
5. I would like to request the embargo of my thesis for 24M from the submission date due to conference/journal publication process and procedures

Student's Full Name & Signature:

Syeda Prima Tasnim
16366008

Approval

The project titled “A framework of biometric recognition and personalized mobile application to establish a dynamic connection with the ATM to enable secure transaction. ” submitted by

- Syeda Prima Tasnim: 16366008

of Summer,2019 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of M.Engg in Computer Science & Engineering on 28 August, 2019.

Examining Committee:

Supervisor:

_____

Md. Khalilur Rahman, Ph.D.
Associate Professor, Department of Computer Science & Engineering,
BRAC University, Dhaka Bangladesh.

Departmental Head:
(Chair)

_____

Chairperson, Department of Computer Science & Engineering,
BRAC University, Dhaka Bangladesh

Abstract

Secure transaction of money is the prime concern of banking industries for establishing a strong banking network worldwide. By the vast uses of Automated Teller Machine (ATM) in this industry transaction of money has become easier for the customers. But the system needs more secure transaction method for avoiding unwanted incidents. Smart and secure transaction through ATM is the thing people want now a days. For making the transaction through ATM more reliable as well as smart a biometric based system along with an android application has been approached in this research paper. The system consists of a fingerprint-based device which is connected with the ATM software and a personalized mobile application for user. Using the application customer can make a 1:1 connection with the ATM software. For transaction customer can control the account using the mobile application and make transaction command which is also connected with the central server. At the very last stage customer needs to give finger print on the designated device for verifying the account holder's presence during the transaction. In this way the less safe ATM card system can be replaced with a smart and secure system. Testing of the system using a custom-made ATM software along with fingerprint sensor justify the authenticity as well as efficiency of the system.

Keywords—fingerprint sensor, ATM banking, mobile application

Acknowledgement

I would like to thank the almighty for giving me the opportunity and ability to achieve a valuable amount of knowledge in this lifetime and with his blessings, I shall continue to pursue all the good things in my life ahead.

I also thank our supervisor, Md. Khalilur Rahman, Ph.D. heartily for giving me the opportunity to work under his supervision and also for his kind support in making this research successful.

I thank BRAC University for giving me the opportunity to be a part of it and all the faculty members who have taught and motivated me to think more deeply.

I thank Information and Communication Technology Division, Bangladesh for giving me the fellowship opportunity to complete the research.

Finally, I would like to thank all the seniors and juniors who have helped in minute tasks, especially Md. Zahirul Islam and Syed Rhythm Ahir Hussain for their support and co-operations.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Introduction

Services related to banking is used by most of the people worldwide. With the help of emerging technologies people can now enjoy the banking facilities for twenty-four hours a day. Services like online banking, Automated Teller Machine (ATM) etc. helps the customer to use transaction services without thinking about the banking hours. For cash transaction ATM is the vastly used system in the whole world. Using a designated ATM card people can easily withdraw cash money from wherever they want. With this very much useful service there are also chance of facing unwanted incidents like hacking passwords of ATM cards and many more. For avoiding these types of incidents more secure and smart transaction system needs to developed.

In the current ATM system using a card anyone can withdraw cash from someone's account if he has the ATM card pin. As password-based system can be hacked so people can face unwanted problems if they lost their ATM card or their ATM card pin. For securing ATM based transaction system there needs to introduce more authentic and complex verification system for avoiding undesired loose. With a vast scope of research and development the topic has been selected for this research paper.

Biometric based authentication is getting popular day by day. As this type of system verify the biological data which is unique for every person so it can secure any system rather than any password-based technique. With the thought of implementing this biometric based authentication system for securing ATM based transaction a fingerprint recognition-based system has been approached in this research paper. In the proposed system a custom-made

finger print device has been connected with the ATM. Using a custom designed personalized mobile application people can easily establish a 1:1 connection with the ATM machine via Bluetooth communication facilities into the fingerprint device. The mobile application is also connected with the central server. So, using the mobile application people can easily make command of transaction but before the final confirmation they need to give the fingerprint in the designated device so that the system can make a credible authentication of the account owner. This type of systems can replace the pin-based ATM card system to secure the banking transactions.

1.2 Literature Review

Investigating related works which has been done previously enrich our knowledge about the topic and give us the scope of research and updates on the designated topic. For this research a couple of related works has been explored. In the research paper [1] an Aadhaar card number based biometric log in system has been described for internet banking in India. Aadhaar card is basically a national Identity card and every citizen has a unique ID number which carries biometric information about the card holder. In the next research paper [2] a face scanning ATM system has been approached where the system only allows the transaction when it can scan the customers face. In the research work [3] a fingerprint based biometric authentication system has been proposed for managing multiple bank accounts for a single person. In this system client can access multiple bank accounts through their unique fingerprint. In the next research work [4] a biometric based secure approach has been proposed with SMS services which uses J2EE technology. After analyzing all these related research works it can be said that there are different approaches taken by many researchers for introducing biometric based authentication system for banking industry. In this research a biometric fingerprint-based system is also proposed with a custom designed personalized

mobile application which can control the command instead of ATM cards and this differentiate the research from other research works.

1.3 Reasons for problem selection

The banking security systems we have right now, do they all provide the security to its maximum capacity? Are we still not facing a lot of problems in terms of keeping our banking secure and easy? In my perspective currently, the banking system is at risk. We use ATM cards, which is not fully safe. People suffer remembering their pin numbers. Sometime the users have to try several times. At the same time, now we are living in an age, where almost a lot of things are in biometric, the unique identity of any human being. In the very near future, our passwords/pin will be replaced by fingerprints. Using fingerprints recognition instead of pin/password is the next generation security level, but this still didn't get much attention in our country. Hence, I have selected this problem as my topic.

1.4 Research Review

The HSBC Mobile Banking, manages your money on the move and around the clock with this secure Personal Banking app from HSBC. This is an application for mobile banking.

Tap 'n Pay, three layers of security via NFC Card, PIN Number, OTP (One Time Password). The customers go to the nearest agent and pay via NFC card, PIN number and OTP security. Tap 'n Pay is a unique product of Mobility iTap Pay (Bangladesh) Limited. It refers to the 4th generation technology of Mobile Financial Service (MFS) through use of terminal and a near field communication (NFC) based card or any other object integrated with NFC Tag.

I have found a research on the existing global banks which are using biometric in their operations [11]. The list of 121 global banks is given below;

	Bank's name	Country	Biometric	Application
1	Jordan Commercial Bank	Jordan	Iris	Branch banking, ATM, Internet banking
2	Cairo Amman Bank	Jordan	Iris	Branch banking, ATM, Internet banking
3	National Bank of Australia	Australia	Voice	Telephone banking
4	Tallinn Business Bank (TBB)	Estonia	Dynamic Signature	Internet banking
5	Bank Hapoalim	Israel	Dynamic Signature	Branch banking
			Voice	Branch banking, Password/PIN reset
6	First Direct Bank	Israel	Voice	Branch banking, Telephone banking, Password/PIN reset
7	Bank Leumi	Israel	Voice	Password/PIN reset
8	Discount Bank	Israel	Voice	Telephone banking
9	FNB Bank	South Africa	Fingerprint	Branch banking
10	The Credit Bank	South Africa	Fingerprint	Access control (Computer system)
11	Absa Bank	South Africa	Fingerprint	Branch banking
12	Standard Bank	South Africa	Fingerprint	ATM
13	Banco Pichincha	Ecuador	Keystroke	Internet banking
14	Deutsche Bank	Germany	Fingerprint	Access control
15	Sparkasse Bank	Germany	Fingerprint	Access control
16	Dubai Bank	UAE	Hand scan	Access control (Safe deposit)
17	Barclays Bank UAE	UAE	Fingerprint	ATM
18	Banco Azteca	Latin America	Fingerprint	Branch banking
19	Bank of Central Asia	Indonesia	Fingerprint	Branch banking
20	Danamon Bank	Indonesia	Fingerprint	Biometric smart card
21	Bank Negara Indonesia (BNI)	Indonesia	Voice	Password/PIN reset
22	Boundary Waters Bank	USA	Fingerprint	Access control (Computer system)
23	Kroger Bank	USA	Fingerprint	POS
24	InTrust Bank	USA	Voice	Branch banking
25	E*Trade	USA	Fingerprint	Access control
26	American Express	USA	Fingerprint	Access control (Physical)
27	California Commerce Bank	USA	Fingerprint	Access control (Network)
28	Mellon Bank	USA	Fingerprint	Checking the history of individuals
29	Bank of America	USA	Fingerprint	Internet banking
			Face	Branch banking
30	United Banker's Bank	USA	Fingerprint	Internet banking
31	Western Bank	USA	Dynamic Signature	Branch banking
32	First American Bank	USA	Dynamic Signature	Document processing
33	Chase Manhattan Bank	USA	Voice	Branch banking
			Dynamic Signature	Document processing
34	Shearson-Hamill Investment Bank	USA	Hand geometry	Access control(Time and attendance)
35	Chevy Chase bank	USA	Fingerprint	Access control (Physical)
36	First National Bank Group	USA	Fingerprint	Access control
37	Commerce bank of International (IBC)	USA	Fingerprint	Internet banking, Access control (Network)
38	First Tennessee Bank	USA	Fingerprint & Hand geometry	Access control (Safe deposit)
39	Charles Schwab Bank	USA	Dynamic Signature	Branch banking, Document processing
40	Bank of Currituck	USA	Fingerprint	Access control
41	People State Bank	USA	Fingerprint	Checking transaction history
42	Shinkin Bank	USA	Finger vein	Access control (Server room)
43	Bank of Hawaii	USA	Fingerprint & Hand geometry	Access control (Safe deposit)
44	Bank of Utah	USA	Keystroke	Internet banking
45	SunFirst Bank	USA	Hand vein	Access control (Data center)
46	Zions Bank (Zions First National Bank)	USA	Fingerprint & Hand geometry	Access control (Safe deposit)
			Fingerprint	Check Cashing
47	West Texas National Bank	USA	Fingerprint	Check Cashing
48	Texas Bank United	USA	Iris	ATM
49	Somer Trust Bank	USA	Voice	Telephone banking
50	Banco Ambrosiano Veneto	Italy	Iris	ATM
51	Banco Bradesco	Brazil	Voice	Telephone banking, Password/PIN reset
52	Bank Islam Brunei Darussalam (BIBD)	Brunei	Fingerprint	ATM
53	HSBC Bank	UK	Face	Access control (Data center)
54	Lloyds TSB	UK	Voice	Telephone banking
55	United Bank Limited (ULB)	Pakistan	Voice	Branch banking
56	Credicorp Bank	Panama	Fingerprint	Access control (Physical, safe deposit box), Branch banking
57	Western Bank	Puerto Rico	Fingerprint	Branch banking, ATM, Internet banking
58	FirstBank Puerto Rico	Puerto Rico	Hand geometry	Access control (Time& Attendance)
59	Vakifbank	Turkey	Finger vein	ATM
60	Akbank	Turkey	Iris	ATM
61	IsBank	Turkey	Finger vein	ATM, POS
62	Ziraat Bank	Turkey	Hand vein	ATM
63	Mauritius Commercial Bank	Republic of Mauritius	Fingerprint	Access control (Bank building)
64	Industrial&Commercial Bank	China	Dynamic Signature	Workflow automation
65	China Merchant Bank (CMB)	China	Voice	Telephone banking
66	People's Bank of China	China	Face	Access control (Physical, Treasury)
67	Bank of China	China	Fingerprint	Access control (Physical, Time&Attendance)
68	Nanto Bank	Japan	Hand vein	ATM, Branch banking
69	Hiroshima Bank	Japan	Hand vein	ATM, Branch banking
70	Customers Japan Post Bank	Japan	Finger vein	ATM
71	Mizuho Bank	Japan	Finger vein	ATM
72	Bank of Kyoto	Japan	Finger vein	ATM
73	Sumimoto Mitsui	Japan	Finger vein	ATM
74	Resona Bank	Japan	Finger vein	ATM
75	Joyo Bank	Japan	Finger vein	ATM
76	Juroku Bank	Japan	Finger vein	ATM
77	Bank of Fukuoa	Japan	Finger vein	ATM
78	CITI Bank	Japan	Finger vein	ATM
79	Tajima Bank	Japan	Finger vein	ATM

81	Suruga Bank Japan	Hand vein ATM,	Branch banking
82	Shinkin Bank Japan	Hand vein ATM	
83	Ogaki Kyoritsu Bank Japan	Hand vein ATM	
84	Ikeda Bank Japan	Hand vein ATM	, Branch banking
85	Norinchukin Bank Japan	Hand vein ATM	
86	Senshu Bank Japan	Hand vein ATM	
87	Citi Bank Singapore Fingerprint ATM		
88	Pictet&Cie Swiss Face Access control (Building, Time&attendance)		
89	Banco Falabella Chile Fingerprint ATM, Branch banking		
90	Al Rajhi Bank Saudi Arabia Hand geometry ATM		
91	Bank of CostaRica Costa Rica Fingerprint Access control		
92	Woori Bank South Korea Fingerprint Internet banking		
93	BanCafe Colombia Fingerprint ATM		
94	Foreign Trade Bank (FTB) Cambodia Fingerprint ATM		
95	BankMed-Lebanon Lebanon Iris Branch banking		
96	Podkarpacki Bank Spoldzielczy (PBS)	Finger vein ATM	
97	Bank Polskiej Spoldzielczy (BPS) Poland	Finger vein	ATM, Branch banking
98	Reserve Bank Malaysia Fingerprint Biometric card, Online purchase		
99	Bank of Cairo Egypt Fingerprint Branch banking		
100	Misr Bank Egypt Iris Branch banking		
101	Group Financiero Banorte Mexico	Fingerprint ATM	
102	Banco Azteca Mexico Fingerprint Branch banking		
103	Den Norske Bank Norway	Iris	ATM
104	First Bank Nigeria Fingerprint ATM		
105	Royal Microfinance Bank Nigeria	Fingerprint	POS
106	ABN AMRO Netherland Voice Telephone banking		
107	Union Bank of India India Fingerprint ATM		
108	ICICI Bank India Fingerprint Access control (Network, Treasury)		
109	Indian Bank India Fingerprint ATM		
110	Canara Bank India Fingerprint ATM		
111	Oriental Bank of Commerce India Fingerprint ATM		
112	State Bank of India (SBI) India Fingerprint Access control		
113	Central Bank of India India Fingerprint ATM		
114	Reserve Bank of India India Fingerprint ATM		
115	Punjab National Bank India	Fingerprint ATM	
116	Dena Bank India Fingerprint ATM		
117	Andhra Bank India Fingerprint ATM		
118	Syndicate Bank India Fingerprint ATM		
119	HDFC India Fingerprint ATM		
120	Catholic Syrian Bank India Fingerprint ATM		
121	Cooperative Agricultural Bank	Voice & Iris Branch banking, Internet banking, Access control(Time and attendance)	

Table 1: The list of 121 banks using biometric in the world

If we do the mathematics, among the 121 banks around the world, 52% of the banks in Asia uses biometric technology and the second continent is the America with 32%, 9% in Europe, 6% in Africa and 1% in Australia [11]. Shown in fig. 1.

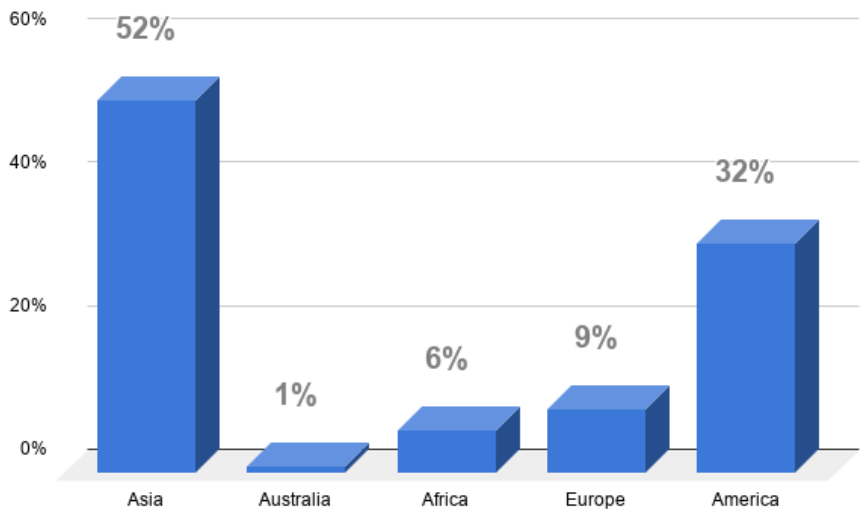

Figure 1: Percentage of Banks using Biometric in the world

Surprisingly, the most used biometric technique which are being used in the world's banks is fingerprint. Approximately 48% of the banks use fingerprint in their different operations. The finger vein pattern and the voice biometric is the next biometric technologies that is being used mostly by the banks with about 12%. Other biometric technologies with less than 10% are respectively: hand vein, iris, signature, hand geometry, face, keystroke and hand scan. [11]

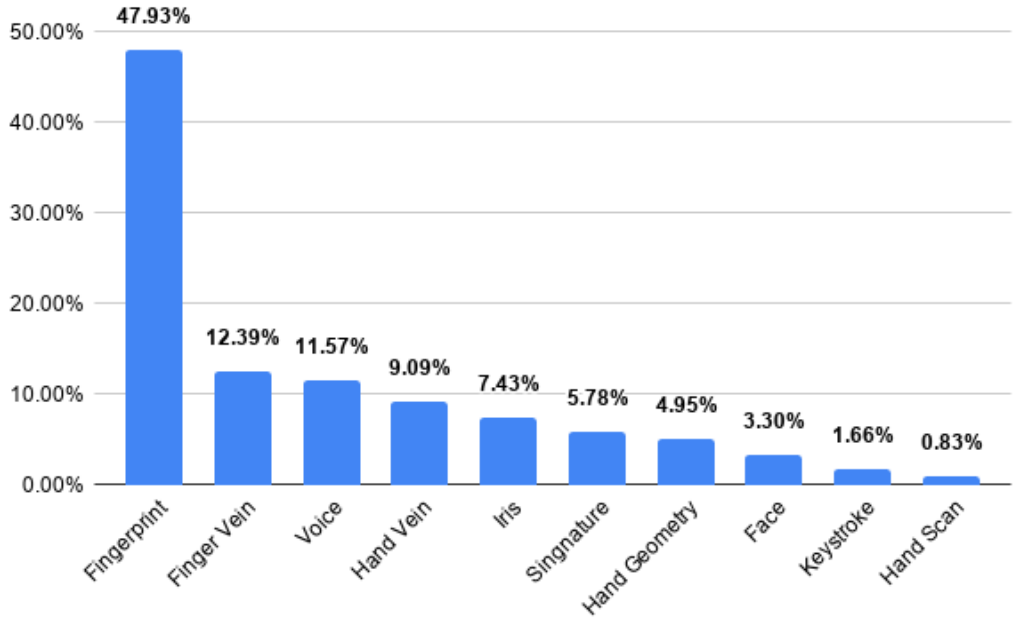

Figure 2: Percentage of biometric techniques being used

Comparison between the fingerprint scanners:

There are three types of scanner: Optical, Capacitive and Ultrasonic scanner.

In old times the Optical and capacitive fingerprint technology creates a 2D scan of the fingerprint. Where the Optical fingerprint is the oldest & uses LED light to capture the image of finger ridges and valleys. While the Capacitive scanner uses electrical signals for the mapping of the fingerprint. And the Ultrasonic uses a very high-frequency ultrasonic sound to creates a detailed 3D model of the scanned fingerprint.

Optical Scanner: As the Optical or capacitive fingerprint technology use light or electronic pulses to create a 2D blueprint of your finger. It is easy to fool an Optical fingerprint sensor by a high-resolution photo or a fake scan of a fingertip. It is also slow as compared to others, there is also a visibility issue for sensors which can result in lower recognition rates in strong sunlight. In term of speed, the optical fingerprint sensor is slowest among others. The Optical finger sensor uses arrays of LEDs as a flash to light up the picture. It captures the picture of fingerprint like a photograph and uses algorithms to detect unique patterns on the surface, such as ridges, marks and analyze the lightest & darkest areas of the image. Nowadays, the Optical fingerprint is also used as In-display fingerprint sensors, in many mobiles like oneplus 6t, vivo,Nokia.

Capacitive Scanner: The Capacitive fingerprint scanner works better than that of optical, it is faster & It is not easy to fool the scanner, as it uses an electric pulse. The Capacitive fingerprint scanner is a bit faster than Ultrasonic fingerprint sensor. The Ultrasonic fingerprint sensor has about 250-millisecond latency for unlocking. The capacitive scanner uses capacitors, which can store electrical charge, also it uses many tiny capacitor circuits to collect data about a fingerprint. On placing a finger on the screen,

the charge in the capacitor will change slightly, while an air gap will leave the charge at the capacitor relatively unchanged. An op-amp integrator circuit is used to track these changes, which is then recorded by an analog-to-digital converter.

Ultrasonic fingerprint sensor: It is best among all, in term of accuracy. It has an error rate of 1%, and can operate through thin materials, such as plastic, glass, or aluminum. It scans through up to 800 µm of glass and up to 650 µm of aluminum and works through dirt, grime, water or even oil. since sound waves can travel through them all. The Ultrasonic hardware consists of a transmitter and a receiver. An ultrasonic pulse placed over the scanner, transmits against the finger, the pulse bounced back to the sensor. Depending upon the ridges & pores, it creates a detailed 3D reproduction of the scanned fingerprint.

Therefore, from the above comparison, we can see that either the capacitive scanner or the ultrasonic scanner can be a good fit for this automation software. Capacitive scanner is accurate, safe and it is good in terms of speed. So, we have chosen capacitive scanner for this research topic.

1.5 Challenges to overcome

In order to develop the entire system, there are many challenges since the entire system has automated machine to machine socket communication and detection. After that verification and finalization. The major challenge will be;

- Detecting real human being: Capacitive scanners is the solution. The system consists of capacitive scanner which ensures the detection of real human being. A capacitive scanner has a capacitor to store little electrical charge in it, which is more difficult to fool. Also, a fake plastic finger will not contain electrical charge in it, as a result the scanner will detect a fake finger.

- Detecting the real time access: The capacitive scanner and a very secure software to detect real time access. The ATM will detect the mobile application once the user establishes a connection. There will be session timeout process which will disable the establishment after a certain time. The user will put his finger on the capacitive scanner, which measures the fingerprint electrically. Instead of creating a traditional image of a fingerprint, capacitive fingerprint scanners use arrays tiny capacitor circuits to collect data about a fingerprint. As capacitors can store electrical charge, connecting them up to conductive plates on the surface of the scanner allows them to be used to track the details of a fingerprint. The charge stored in the capacitor will be changed slightly when a finger's ridge is placed over the conductive plates, while an air gap will leave the charge at the capacitor relatively unchanged. An op-amp integrator circuit is used to track these changes, which can then be recorded by an analogue-to-digital converter. This process will ensure the real time user, because the air gap is not possible with a real time user.
- Machine to machine communication establishment: Automatic socket programming which ensure the detection of the machines (mobile phones) near to the machine (ATM) and collect data from the server about the user who requests access. The socket programming ensures the communication and data transferring between the machines. The machine (ATM) will collect data from the cloud using the existing secure channel and store data itself. the desktop software will be developed in the development process which is an automated fingerprint identification system. In order to transfer data between the machines, it uses restful API within the software. SQLite database, stores the data within the android application, which makes the process easier for the user and also it makes the interface user-friendly

Implementation of fingerprint banking security system faces multiple challenges. Detecting real human being, real time and machine to machine connection are the three major challenge. In terms of solving them, I've come up with concepts and procedures.

Capacitive fingerprint scanners are the popular type which is mostly used in smartphones. The work principle is that if the distance is short enough, it's possible to transfer electricity from a capacitor and the skin. It has capacitor within itself. At the scale of such capacitors, fingerprint ridges are like hills and valleys. Ridges will seem closer to the capacitor, and more electricity will flow away. If you have an array or a grid of capacitors (the more, the higher the resolution), they can act like pixels with varying gray-level intensity (higher electricity flow, darker pixel), thus forming a 2D fingerprint image. It's complex, very robust and only works with skin.

One can't fool it with a piece of paper, and if you try to make a mold of a real fingerprint, you need to find a material that has the same conductivity as skin. Not impossible, but inconvenient enough to weed out most perps.

The downside of capacitive fingerprint readers is that they can't work if the finger isn't clean, or has water/sweat on it because that changes the conductivity upon which the system is built. Also, they don't work behind metal. That's why there's always a visible fingerprint reader.

In order to detect real time human being, capacitive fingerprint scanner is the best concept to use. This scanner works with capacitor which passes electricity. The main advantage of a capacitive scanner is that it requires a real fingerprint-type shape, rather than the pattern of light and dark that makes up the visual impression of a fingerprint. This makes the system harder to trick. Additionally, since they use a semiconductor chip rather than a CCD unit, capacitive scanners tend to be more compact that optical devices

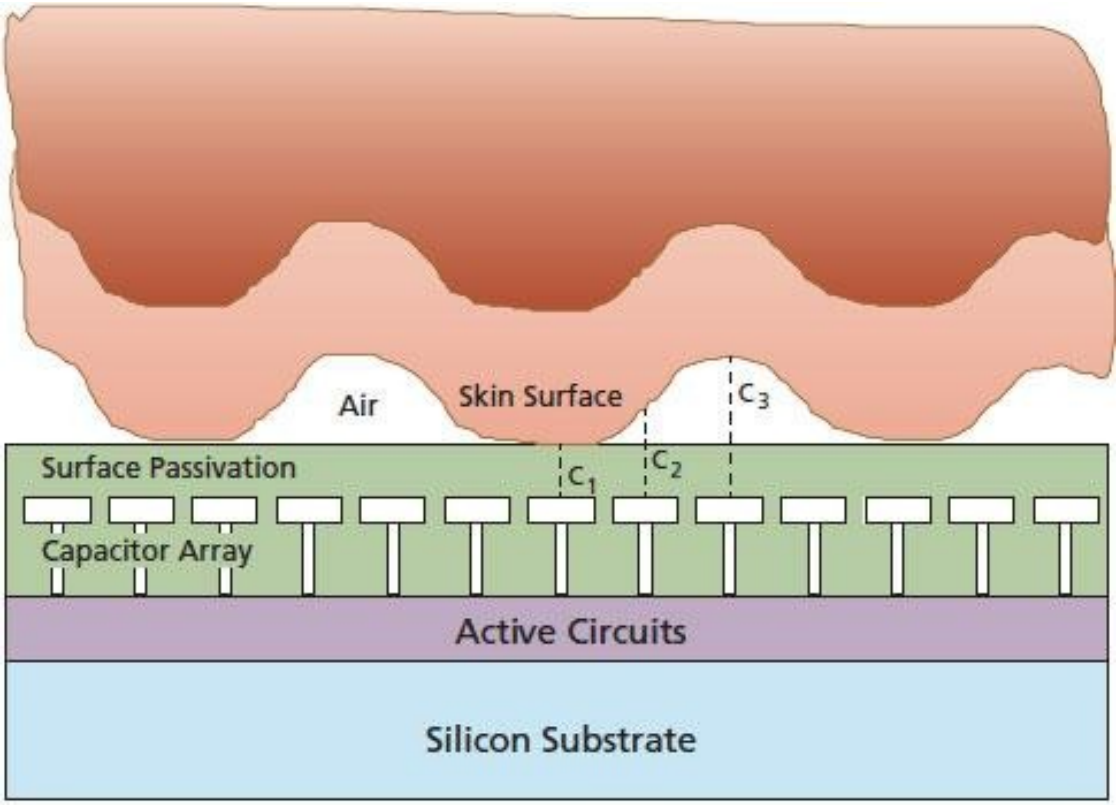

Figure 3: Capacitive Scanner diagram

1.6 Biometric & Banking, why it's difficult?

- Easily hackable/Easy to find - A fingerprint is easy to find. You can get the fingerprints of any specific person from his house/office/car/papers.
- Big repercussions - By any chance if the fingerprint is stolen, then it will be hard to replace and regenerate a new fingerprint, but in text-based password it is easy to regenerate a new password at any time.
- Lack of revocability - Cannot be replaced easily like password, once a fingerprint is associated with a user, it will be a complex process to change it later
- Biometrics aren't for everyone - not for everyone, disable person might not be able to use it, without internet cannot use it, without smartphones cannot use it

The advantages of biometric technology are given below;

1. Biometric technology is very useful for ID verification
2. Accuracy is one of the main advantages associated with biometric technology. The high individual identification accuracy is why a lot of companies use biometrics for their security purposes. Biometrics relies on the use unique physical traits rendering a very accurate technique of authenticating end users.
3. Biometric characteristics cannot be recreated or stolen, biometric systems present a superior level of security
4. It is hard to be damaged or changed. The behavioral and physical elements used for biometric verification such as fingerprints, iris/retina, voice, pulse, DNA, vein, etc. are less in danger to damage and sudden changes.
5. It is less time consuming, dependable, user friendly, hard to falsify, requires negligible training, is inexpensive and accesses distinctive recognition features of individuals resulting in accurate verification.
6. Biometric technology can be used in a lot of industries, means the same concept can be reproduced for security and accuracy
7. It can be effectively used in forensics. This technology can be utilized for criminal identification and prison security.
8. Biometric technology can meet the increased requirement for accurate verification when accessing accounts, it turns out to be the best and most suitable solution for secure mobile transaction identification.
9. It can be used to access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks etc.
10. With biometrics technology, fingerprints won't be lost and can't be attained by someone else. You do not have to remember and write down the fingerprints like password/PIN.

1.7 Proposed solution to the problems

- Fingerprints are easy to get, but my proposed system is very complex and uses very secure software, as a result it will not be possible to get access to the account even if

you know the fingerprints. My system will detect plastic or any other no-realistic finger very easily, it will detect if the finger is not real time also.

- The reason behind introducing fingerprint banking system is to ensure that the user have uniform identity, which will never be repeated. This system can perform more secure than the existing system where people use passwords to get access to their account.
- Again, the secure software will ensue that you do not have to change it frequently. This biometric system is the ultimate secure channel and ensures secure money transfer in a very short time.

Therefore, this automation includes capacitive fingerprint scanner which will detect a real time fingerprint image. The 1:1 connection between your mobile phone and the ATM will ensure secure connection and identify the user even before the user puts the fingerprint. The mobile application will be real time synced with the server, which ensures the security of the user profile and the account.

Chapter 2

System Analysis and Research Methodology

2.1 System Analysis & Design

Analyzing biological data for authentication is safe and credible option than any password-based authentication system. With the motive of developing a biometric smart authentication

system for banking industry a fingerprint based complex authentication system has been proposed in this research.

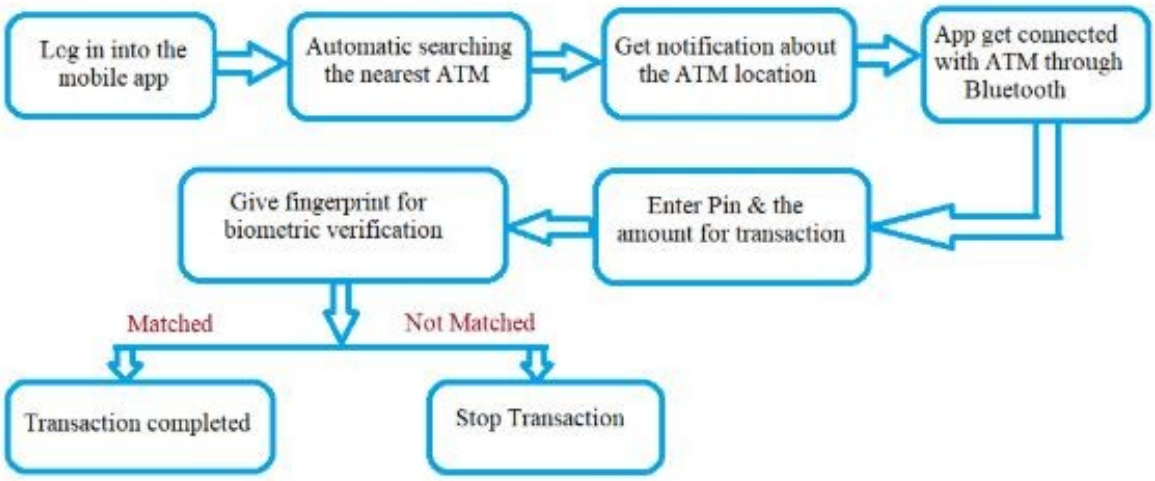

Figure 4.1. Complete System Block Diagram

The flow diagram of the prototype [figure 4 .1] is given above. There are six steps to complete the entire process and successfully exchange money between the account holder and the bank account. This is the most challenging part in my thesis. The six steps are described below;

1. Establish 1:1 connection with the ATM, send account_id to the ATM and receive atm_id from the ATM
2. Input account_id from the user through the UI of the mobile application
3. The ATM establishes connection with the server and use the secure channel to identify the user and collect data from the server
4. Take input of fingerprint from the user using the capacitive scanner through the ATM machine
5. Compare the two-fingerprint received from the central server and the ATM scanner input
6. If matches, send acknowledgement to the server with data and enable access (atm_id and device_id,acount_id)

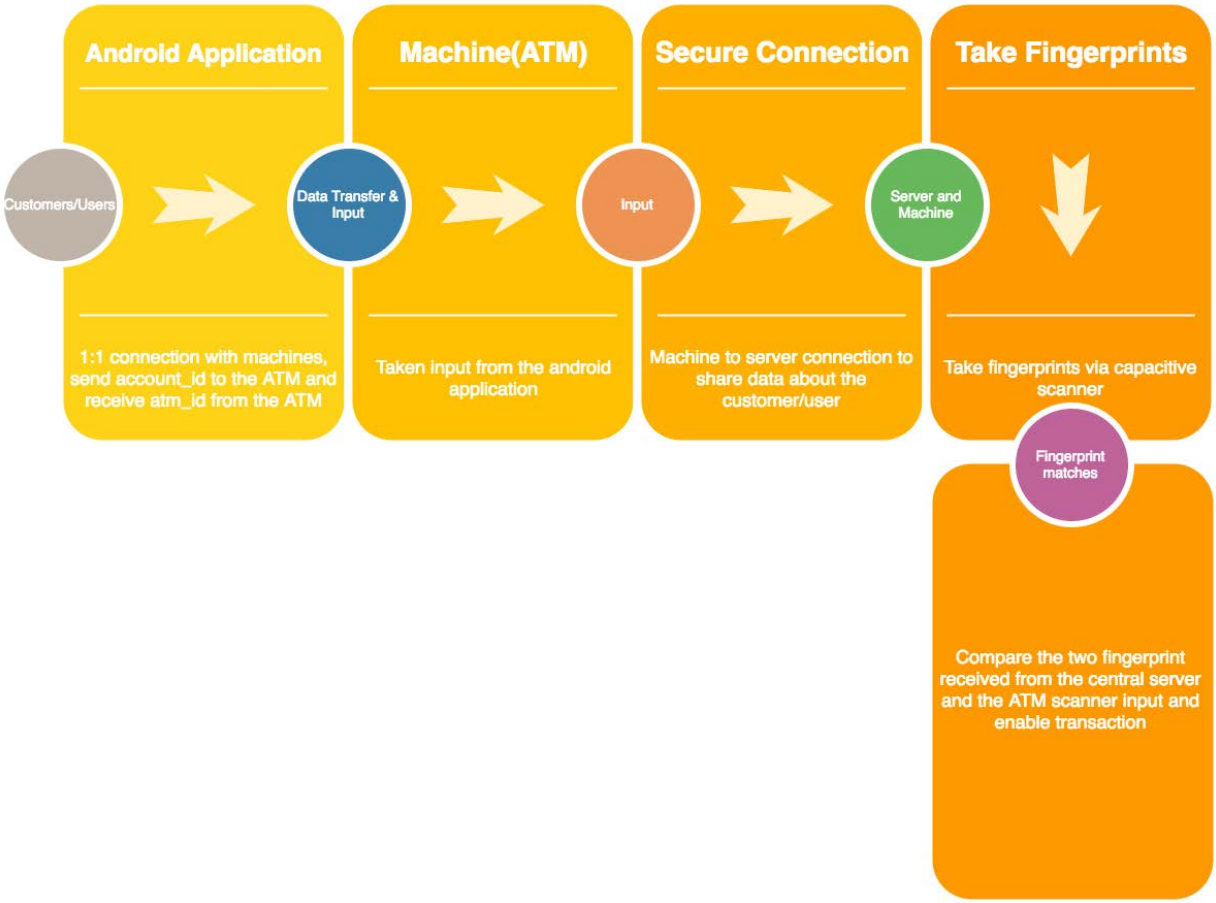

Figure 4.2. Information flow Diagram

As discussed above 1:1 connection with the ATM will be done in a secure channel. After the connection is established, it will share its id from the database and sync with the user.

Once a user comes within a network of an ATM machine, it will auto establish the connection. Every customer/user will have an android application installed in their phone, on the other hand every ATM machine will have desktop software installed in their CPU. This two software will exchange ids within themselves through API. The first connection will be established at that moment. The ATM machine will detect the customer/user's unique id, if that matches with its central server then the first 1:1 connection will be established. In the second step, the customer/user will input account_id in the given mobile application through its user interface. The ATM then will establish a connection with the server and use the secure

channel to identify the user and collect data from the server regarding that user. In the third step, the customer/user will insert fingerprints into the machine. The ATM machine will have capacitive scanner integrated in it.

Capacitive fingerprint scanners generate an image of the ridges and valleys that make up a fingerprint. But instead of sensing the print using light, the capacitors use electrical current.

In the capacitive fingerprint scanner, the sensor is made up of one or more semiconductor chips containing an array of tiny cells. Each cell includes two conductor plates, covered with an insulating layer. The cells are tiny -- smaller than the width of one ridge on a finger. The functions of capacitive scanner is discussed more in this paper section 1.4

The ATM receives the fingerprint from the customer/user via capacitive scanner, as it has already stored the customer/user's data earlier from second step, now it matches two of the fingerprints, the one which it has received from the capacitive scanner and the second is from the customer's profile via secure channel from data server. All of the connection will happen within a secure channel of APIs.

Finally, if the fingerprint matches, the ATM will give access of the account to the customer/user and will let the customer/user make transactions. The mobile device will connect with the nearest free channel.

There are several challenges to face to secure the channel. This system will choose one existing secure channel, which is being used for the ATM machine, but it will enable the new era of banking security system by enabling easy and reliable banking. Biometric banking security system is not new, but secure fingerprint recognition for banking is a unique concept. I have introduced two layers of security; in first step the 1:1 connection between the android mobile app and the ATM machine and in second step the connection happens between the android mobile application and the data server via ATM machine.

2.2 Methodology

Collecting biometric data from the customer and sending those data to the central server is an important task for this system. For ensuring a structured process of biometric data collection a custom designed software has been developed named the ATM admin software using C# programming language. In the software customer can submit bank account number, pin number and the fingerprint. After collecting the data from the customer, the software automatically generated a folder in the central server and save those data. By using this software authority can input data regarding the existing ATM booths. ATM booth's GPS location, address and

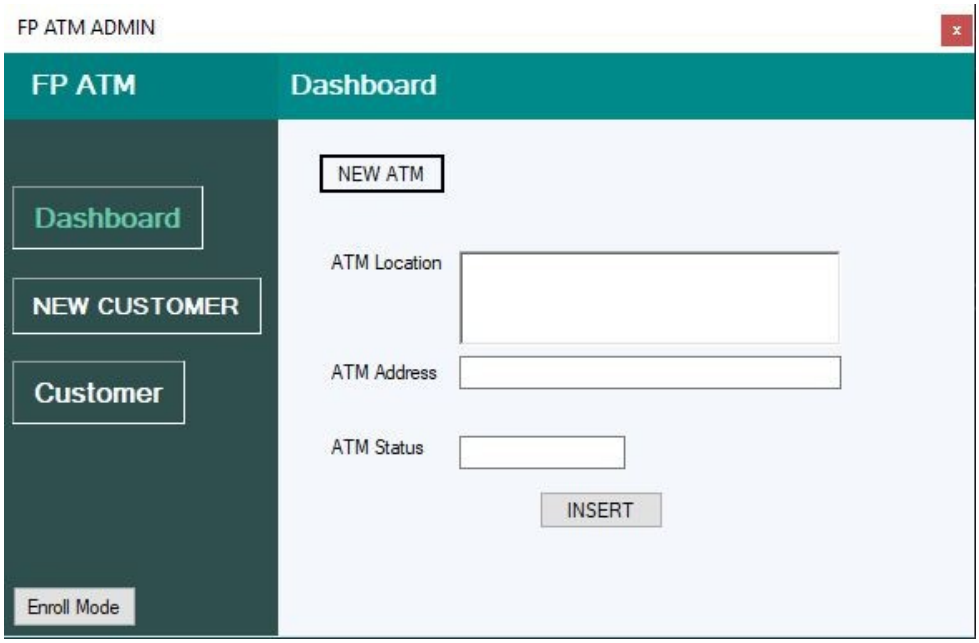

Figure 5.1 Customer Data collection

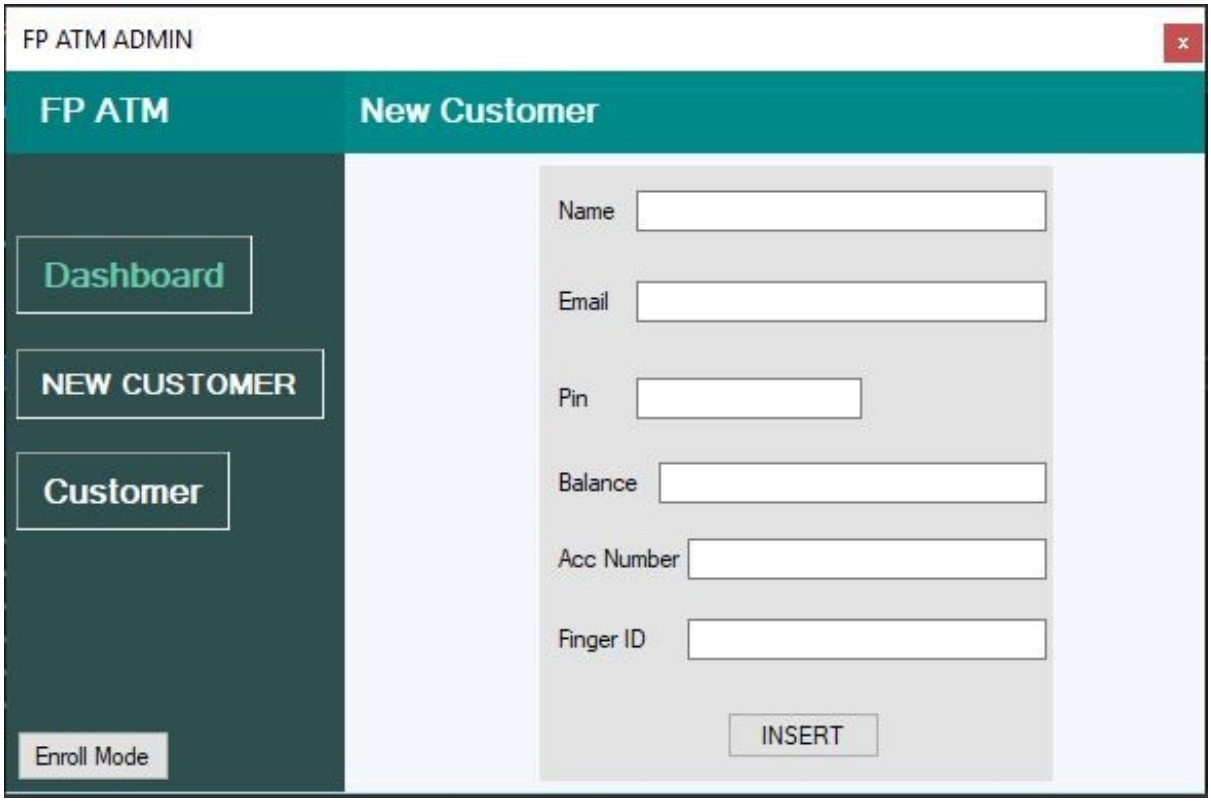

Figure 5.2 Data regarding ATM

status can be added into the central server as input through this software [9].

When any customer logs in into the mobile app then it can automatically start searching for the nearest ATM booth. In this process Haversine formula[10] has been applied for calculating the shortest path. For navigation this formula works as a vital equation [06] and works with maximum accuracy [05]. Conventionally Haversine formula has been used for calculating the distance between two coordinates on a sphere. From [07] [08] the conventional equation of the popular Haversine formula is

Haversine (θ) = 〖sin〗^2 θ/2 … (1)

Using this the distance between two coordinates for radius r can be calculated through

d=2r 〖sin〗^(-1) √(〖sin〗^2 ((α_2-α_1)/2) +cos (α_1) cos (α_2) 〖sin〗^2 ((β_2-β_1)/2)) ……. (2)

Here r is the radius of the earth and α, β are the latitude and longitude respectively. Based on the two equation a location-based recommendation algorithm has been developed [5]. In this algorithm input will be the customer's location (latitude and longitude) and couple of ATM booth locations which can be acquired from the central server. Then an array has been initialized for storing the interspace values between customer and the ATM booth. For example, If the system takes 3 ATM booth location a1, a2, a3 and a single customer location C then it will calculate the interspace for customer location vs each ATM booth location separately using Haversine formula and store the final value in the array I. Then the system will place all the resultant values in ascending order. After that a map will be generated with all the A locations and the nearest ATM booth location will turn Green as per customers closeness.

***Algorithm**: Location Based Recommendation Algorithm*

Input:

Customer's location (latitude and longitude) C (α_1, β_1)

Multiple ATM Booths location (latitude and longitude): A = [a1 (α_2, β_2), a2 〖(α〗_3, β_3), a3 〖(α〗_4, β_4)]

Output:

Values of interspaces between customer and all the ATM booths location categorized in ascending order according to customers adjacent.

Steps:

Initializing: Array I

For every a in A,

- Calculate the interspace between C and a using Haversine formula.

- Store the interspace values in I

Categorized the array I in ascending order

Generate a map including all the A locations and separate the nearest location based on closeness of C locations.

Chapter 3

System Implementation

The total system has been divided into three primary subsystems. The subsystems are as follows- Fingerprint Device, Mobile Application, ATM Software.

3.1 Fingerprint Device

The Designing a fingerprint device for collecting biometric data from the client is the first step of this research. As the device needs to be fit for the present ATMs that's why a design has been chosen with omnipresent configuration so that it can configure itself with the existing machines. The device consists of three major components which are an optical fingerprint sensor, microcontroller board Arduino Uno with microchip ATmega328P and a Bluetooth module. The total device needs to be compact so that it can be easily placed on the ATM. Every module has been chosen under the consideration of building a robust device. The developed device shown in Fig. 5 is connected with a central server through the ATM software.

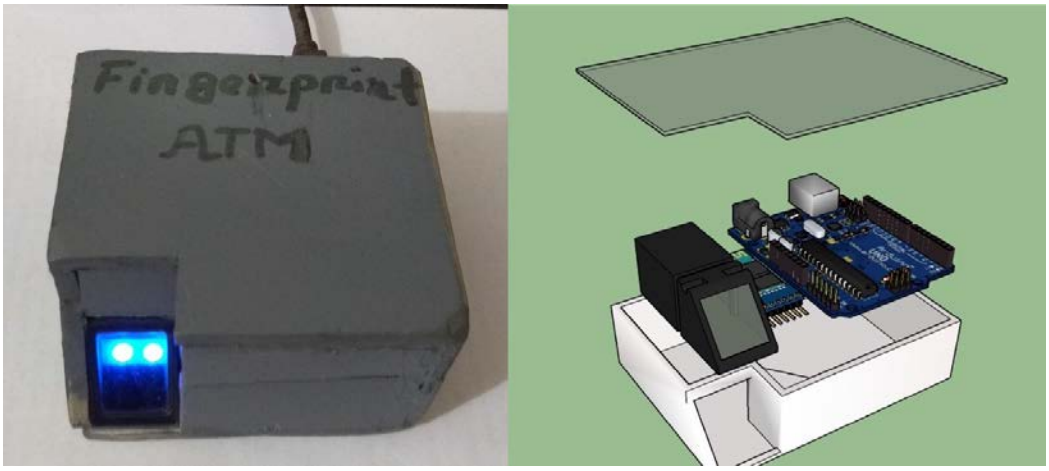

Figure 6. Original Device and 3D CAD Model

3.2 Mobile Application

The second step of this research is to develop a custom designed mobile application for the customers. As android operating system is more popular and user friendly that's why android studio has been used for designing this mobile application. User needs to log in into the application using a user ID and a password.

This mobile app can automatically search the nearest ATM booth and get connected with an ATM when the phone maintains a specific distance using the Bluetooth option of the phone. Through internet the application is get connected with a central server management. A user-friendly graphical user interface has been created for the customers shown in Fig. 6.

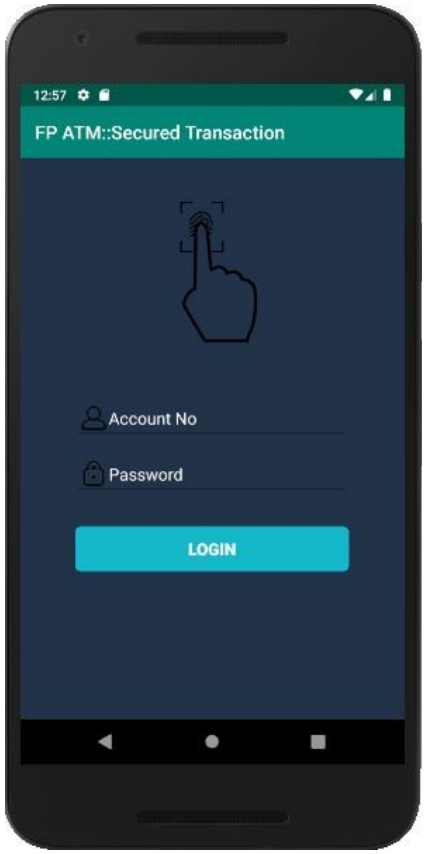

Figure 7. Graphical User Interface of mobile application

3.3 ATM Software

The developed fingerprint device needs to get connected with an ATM for processing any transaction. In this case for test purpose a desktop software has been developed which can behave like a real-life ATM shown in Fig. 7. For developing this software C# programming language has been used. The graphical user interface has been developed in a way that user can get real life experience of using a real ATM. This software is also connected with the central server. From fast cash option to balance inquiry option even fund transfer option has been included into the desktop software. User can easily control the movement of this desktop software using the personalized mobile application.

Each element of this total system is dependent on one another. For completing one single transaction each part of this system needs to work properly. If one single section of the

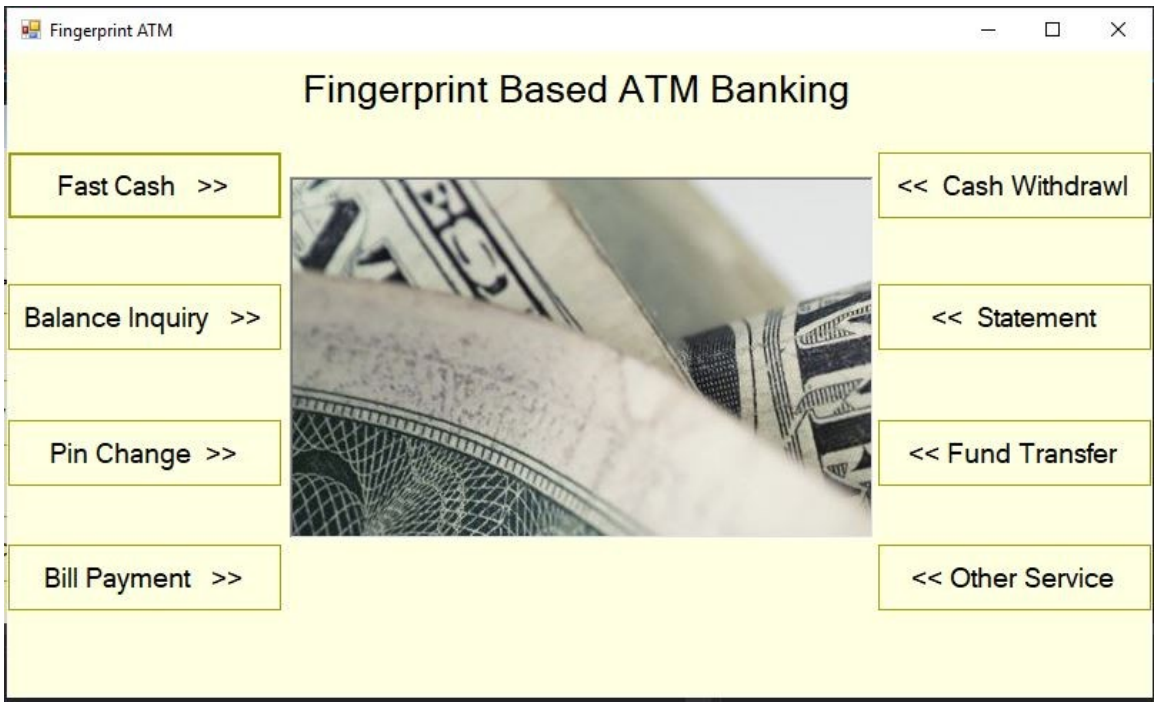

Figure 8. Graphical User Interface of desktop ATM software

system is missing then the transaction process will not work. Using this type of complex verification proper authentication can be ensured.

Chapter 4

Experimental Analysis

Testing the developed system in real life is the way to justify the accuracy and reliability. In this case there are two types of experiment have been conducted for verifying the system. First

one is the testing of search algorithm, where finding the nearest ATM booth in the customized mobile application using Haversine formula-based algorithm has been tested. Three different ATM booth coordinates and a user coordinate from the place Mohakhali, Dhaka -1212, Bangladesh has been used as input in the algorithm. When the user turns on the mobile application then it automatically searches the nearby ATM booth. The application suggests the nearest ATM booth using the algorithm values by turning the atm location identifier into green. In this process the algorithm successfully detected all the three ATM booths and suggested the nearest ATM booth to the user show in Fig. 9.1 and 9.2.

Secondly, with real ATM there are a lot of sophisticated and confidential data connected to the system, that’s why bank authorities did not give the permission to test the developed device with a real ATM. As there are restrictions about this issue so the device had been tested using the custom designed ATM software in a local machine. The ATM software works as a real-life ATM which will respond to the commands through showing some specified notes on the monitor. So, the fingerprint device has been connected with the ATM software via a desktop computer. The ATM software has been named ATM machine and the location of

the ATM has been selected as Mohakhali, Dhaka-1212, Bangladesh. When the user turns on the mobile application then it automatically gets connected with the ATM software using Bluetooth shown in fig 10. After placing the pin and the amount when the user gave the fingerprint on the designated device which is connected with the ATM software then a note “Transaction Completed” has been shown in the ATM software graphical user interface in Fig. 11. In this way the developed fingerprint device and the ATM software has been tested successfully.

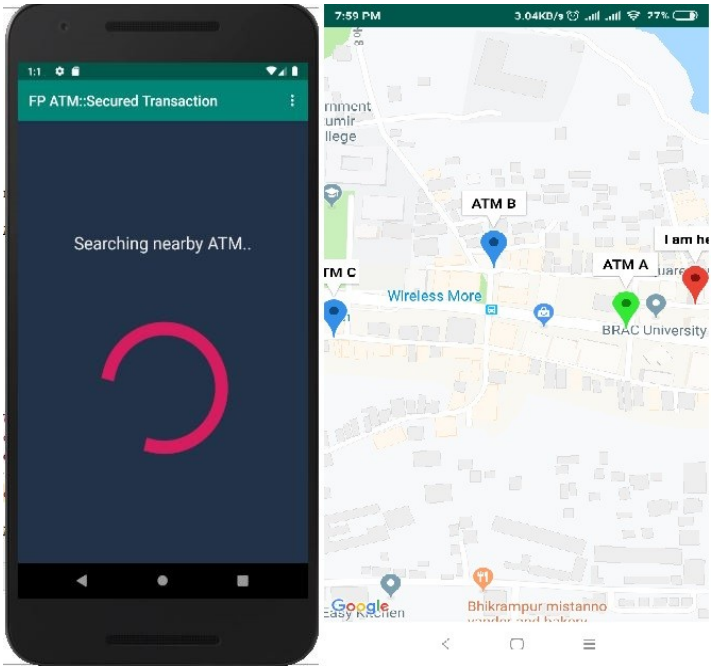

Figure 9.1 Automatically searching nearby ATM. 9.2 Generated Map using the location-based algorithm

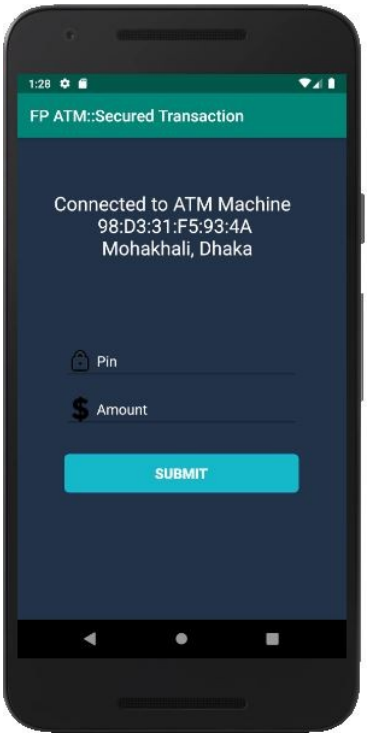

Figure 10. Building connection with the ATM software through mobile application

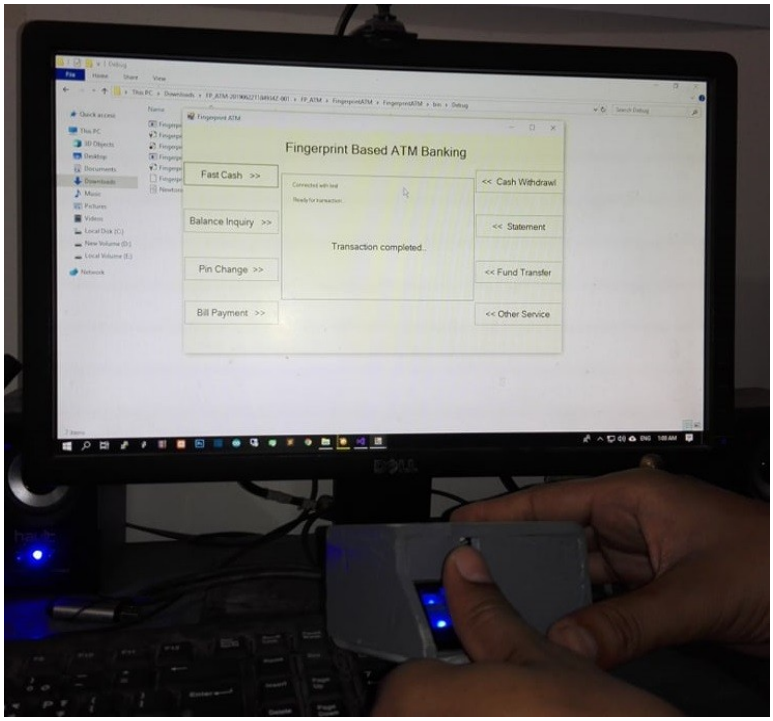

Figure 11. Successful completion of transaction

Table 2. Experiment Result

Experiments		
1. Search Algorithm Test		
Search between ATM booth locations	**Detection of ATM booth locations in map**	**Detection of nearest ATM booth location in map**
3	3	1
2. Transaction Test in ATM Software		
Mobile application connection with Fingerprint Device	**Applying pin, amount & finger print as input**	**Transaction Status**
Successfully Established	Successfully Received by the Device & the ATM Software	Transaction Completed Successfully

Chapter 5

Conclusion

5.1 Concluding the research

Utilization of biometric based authentication systems in the banking sector is getting more popular. For this type of system clients can enjoy secure transaction than past times. In this research a total banking authentication system has been introduced and developed. Fingerprint based biometric data collection device makes the system smooth. The location-based algorithm ensures successful tracking of nearest ATM booths for user. Different custom designed software makes the data collection and testing process easier. In the near future the system can be modified for fulfilling all the requirements so that it can be tested with real ATM. Collection of data can be increased for covering a large area and a large number of customers. If all the modification can be done then this type of system can protect us from unwanted situation during transaction and people can enjoy carefree banking services.

5.2 Future Work

In this research I have found a lot of scope of improvements in the automation software in order to make the software more effective. So, in the future I will implement artificial intelligence for searching the nearest ATM in the shortest time possible. I intent to work

towards minimizing the total transaction time for a user in the ATM. I can optimize the time by implementing AI for shortest path available. At first, I will take all of the ATM in Dhaka City as a knowledge base and implement the AI to find the nearest ATM in the shortest possible time, eventually the entire country and the world.

References

[1] P. K. Saralaya, R. Anjali and N. V. Reddy “Biometric Authentication usage for InternetBanking” in the proceedings of IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), pp. 1-5, May 2017.

[2] A. V. Bataev “The Model of Assessing Economic Efficiency of Biometric ATMs” in the proceedings of IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp. 1-6, January 2019.

[3] A. Taralekar, G. Chouhan, R. Tangade and N. Shardoor “One Touch Multi-banking Transaction ATM System using Biometric and GSM Authentication” in the proceedings of International Conference on Big Data, IoT and Data Science (BID), pp. 1-5, December 2017.

[4] R. Alaoui, K. Abbad, A. EL. Alloui and M. A. Kassimi “Secure approach for Net

Banking

by using Fingerprint Authentication in Distributed J2EE Technology" International Journal of Computer Science and Information Security (IJCSIS), ISSN-1947-5500, Vol. 14, No.7, July 2016.

[5] H. Mahmoud and N. Akkari, "Shortest Path Calculation: A Comparative Study for Location-Based Recommender System" in the proceedings of World Symposium on Computer Applications & Research (WSCAR), pp. 1-5, December 2016.

[6] D. P. v. Ingole and M. M. Nichat , "Landmark based shortest path detection by using Dijkestra and Haversine Formula," International Journal of Engineering Research and, India, 2013.

[7] S. Omatu, J. Neves, . J. . M. C. Rodriguez, J. F. P. Santana and . S. . R. Gonzalez, Distributed computing and artificial intelligence: 10th International Conference, New York: Springer Cham Heideberg, 2013.

[8] ElinaAgapie.jason Ryder, Jeff Burke, Deborth Estrin, ”Probable Path Interference for GPS traces in cities”, university of California,2009.

[9] K.M.Chandy,J. Misra, “Distributed Computation on Graphs: Shortest Path Algorithm”, University of Texas, March 1982.

[10] C. N. Alam, K. Manaf, A. R. Atmadja and D. K. Aurum “Implementation of Haversine Formula for Counting Event Visitor in The Radius Based on Android Application” in the proceedings of 4th International Conference on Cyber and IT Service Management, pp. 1-6, April 2016.

[11] Hosseini, Seyyede Samine & Shahriar Mohammadi, Dr. (2012). Review banking on biometric in the world's banks and introducing a biometric model for Iran's banking system. JBASR. 2. 9152-9160.