VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"JNANA SANGAMA", BELAGAVI -590 018.

2020 – 2021

A Project Report
(Phase - I)
on

"Remote Authorization for ATM Transactions using Fingerprint and T-OTP"

Submitted in partial fulfillment for the award of the degree of
BACHELOR OF ENGINEERING
in

ELECTRONICS & COMMUNICATIUON ENGINEERING

Submitted By

SHREYAS.G[1JB17EC085] **SHREYAS.M.O[1JB17EC086]**
SUMANTH.T.P[1JB17EC090] **TEJAS MUTHYA[1JB17EC095]**

Under the guidance of

DR. K V MAHENDRA PRASHANTH
Professor and HOD, Dept. of ECE

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

SJB INSTITUTE OF TECHNOLOGY

#67,B G S HEALTH AND EDUCATION CITY
Kengeri, Bengaluru-560 060.

||Jai Sri Gurudev||

Sri Adichunchanagiri Shikshana Trust®

SJB INSTITUTE OF TECHNOLOGY

BGS Health & Education City, Kengeri, Bengaluru-560 060.

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

CERTIFICATE

Certified that the project work phase – I entitled **"***Remote Authorization for ATM Transactions using Fingerprint and T-OTP***"** carried out by **Shreyas.G[1JB17EC085], Shreyas.M.O[1JB17EC086], Sumanth.**T.P**[1JB17EC090] and Tejas Muthya[1JB17EC095]** are bonafide students of **SJB Institute of Technology** in partial fulfilment for the award of **"BACHELOR OF ENGINEERING"** in **ELECTRONICS AND COMMUNICATION ENGINEERING** as prescribed by **VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI** during the academic year **2020 – 21**. It is certified that all corrections/suggestions indicated for internal assessment have been incorporated in the report deposited in the departmental library. The project report has been approved as it satisfies the academic requirements in respect of project work phase – I prescribed for the said degree.

Dr. K V Mahendra Prashanth	**Dr. K V Mahendra Prashanth**	**Dr. Ajai Chandran C K**
Professor & Head	**Professor & Head**	**Principal**
Dept. of ECE, SJBIT	**Dept. of ECE, SJBIT**	**SJBIT**



ACKNOWLEDGEMENT

We would like to express our profound grateful to **His Divine Soul Jagadguru Padmabhushan Sri Sri Sri Dr. Balagangadharanatha Mahaswamiji** and His Holiness **Jagadguru Sri Sri Sri Dr. Nirmalanandanatha Swamiji** for providing me an opportunity to be a part of this esteemed institution.

We would also like to express our profound thanks to **Revered Sri Sri Dr. Prakashnath Swamiji,** Managing Director, SJB Institute of Technology, for his continuous support in providing amenities to carry out this project (Phase – I) in this admired institution.

We express our gratitude to **Dr. Ajai Chandran C K**, Principal**,** SJB Institute of Technology, for providing me excellent facilities and academic ambience; which helped me in satisfactory completion of project work (Phase – I).

We extend our sincere thanks to **Dr. K V Mahendra Prashanth**, Professor & Head, Department of ECE; for providing us invaluable support throughout the period of my project work (Phase – I).

We wish to express our heartfelt gratitude to my guide, **Dr. K V Mahendra Prashanth**, for his valuable guidance, suggestions and cheerful encouragement during the entire period of my project work (Phase – I).

We express my truthful thanks to **Dr. Mahantesh K & Mr. Bhaskar B,** project coordinators, Dept. of Electronics and Communication for their valuable support.

Finally, We take this opportunity to extend my earnest gratitude and respect to our parents, teaching & technical staff of the department, the library staff and all my friends, who have directly or indirectly supported me during the period of my project work (Phase – I).

Regards,
Shreyas.G,Shreyas.M.O,
Sumanth.T.P , Tejas Muthya

DECLARATION

We hereby declare that the entire work embodied in this project report has been carried out under the supervision of **Dr. K V Mahendra Prashanth,** Professor and HOD, Department of ECE, SJBIT in partial fulfilment for the award of "BACHELOR OF ENGINEERING" in ELECTRONICS AND COMMUNICATION ENGINEERING as prescribed by VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI during the academic year 2020 – 21.

Shreyas.G [1JB17EC085]
Shreyas.M.O [1JB17EC086]
Sumanth.T.P [1JB17EC090]
Tejas Muthya[1JB17EC095]

Abstract

The intention of our project is similar to what the intention of every good project should be. It is to solve an existing drawback in the system. We have set out to create a Remote Authorization using a time-based OTP and fingerprint scan, so as to create a two-stage verification. We also aim to counter certain other small issues that exist in practice now. The existing technology uses a less secure 4-digit PIN and has a single stage verification. There's also an added drawback of a card being limited to a single bank account. A team at SBI has proposed a Remote Authorization that requires ATM scanners to be included in every ATM. This would cost a lot of overhead to the authorities in terms of acquiring scanners and installing it in large number of ATMs. We have come up with a project that uses a unique time-based OTP and also gives an option of fingerprint scan. The smart card that we provide can be linked to multiple accounts. A dedicated android application and a server will be set up to facilitate smooth transactions.

Table of Contents

List of figures

List of Tables

CHAPTER-1

INTRODUCTION

An Automated Teller Machine (ATM) allows customers to perform banking transactions anywhere and at any time without the need of human teller. By using a debit or ATM card at an ATM, individuals can withdraw cash from current or savings accounts, make a deposit or transfer money from one account to another or perform other functions. A person can also get cash advances using a credit card at an ATM. Individuals should be aware that many banks charge transaction fees generally ranging from Rs.50- 150 per transaction for using another bank's ATM.

Figure 1.1 Automated Teller Machine

The ATM is online with the bank, that is, each transaction will be authorized by the bank on- demand and directly debited from the account's owner. The ATM works as follows. First, the client will insert his/her client card in the ATM and then the ATM will ask for a Personal Identification Number (PIN), if the number is entered incorrectly several times in a row, most ATMs will retain the card as a security precaution to prevent an unauthorized user from working out the PIN by pure guess work. Once the correct PIN is given, the ATM will ask for the amount of money to be withdrawn. If the amount is available and if the client has enough money on his credit then the said amount of money will be paid. Whether the amount of money is payable or not, i.e. the ATM has enough cash but could be the case the ATM has no change for that amount, will be also checked. Once the money is offered to the client a countdown is started, i.e. the client has a determined amount of time to pick up the money. If this time-out is over, the money will be collected by the ATM and the transaction will be rolled back.

There are also many "phantom withdrawals" from ATMs, which banks often claim are the result of fraud by customers. Phantom withdrawals are considered to be a problem generated by dishonest insiders by most other observers.

1.1 Background

At the time (1968) Wetzel was the Vice President of Product Planning at Docutel, the company that developed automated baggage-handling equipment. The other two inventors listed on the patent were Tom Barnes, the chief mechanical engineer and George Chastain, the electrical engineer. It took five million dollars to develop the ATM. The concept of the modern ATM first began in 1968, a working prototype came about in 1969 and Docutel was issued a patent in1973. The world's first ATM was installed in Enfield Town in the London Borough of Enfield, London on June 27 1967. The first working ATM was installed in a New York based Chemical Bank.

The first ATMs were off-line machines, meaning money was not automatically withdrawn from an account. The bank accounts were not (at that time) connected by a computer network to the ATM. Therefore, banks were at first very exclusive about who they gave ATM privileges to. Giving them only to credit card holders (credit cards were used before ATM cards) with good banking records. Wetzel, Barnes and Chastain developed the first real ATM cards, cards with a magnetic strip and a personal ID number to get cash. ATM cards had to be different from credit cards (then without magnetic strips) so account information could be included.

1.2 Existing Systems and their Drawbacks

On most modern ATMs, the ATM card used by the customer for each bank account which is a plastic ATM card with a magnetic stripe or a plastic smart card with a chip. However, password PIN which is the main authentication for ATM transactions represent the weakest link in the computer security chain. ATM is an electronic device which provides the user to perform transactions without the need of cashier, bank teller. ATM services are popular because of their easiness for banking systems. In modern ATMs, the customer account can be identified by inserting a plastic card with magnetic strip that contains account number. The customer then verifies identity by entering a pass code i.e. personal identification number

1.3 Proposed System

The idea behind this project is to provide better security for ATM transactions through double authentication through Fingerprint Authentication and One Time Password (OTP).
The hardware used to achieve this objective is a Raspberry Pi and an RFID Card Reader. A server will be hosted along with a mobile application which will be used for communication between the user and the server. As soon as the user enters the ATM and swipes his/her credit or debit card followed by the entry of the desired amount, the server sends a request to the mobile application where the user will have to respond by scanning his/her fingerprint. The application sends an OTP to the server which will be used by the server for verification of the user, thereby completing the two-stage authentication process.

1.4 Advantages of the proposed system

ATMs for easy, quick and multiple access to user's accounts with enhanced security. Users can access multiple accounts using a single ATM card to conduct different banking transactions. The advantages of proposed system are,

- High level security with two factor authentication.
- It's not possible to duplicate RFID cards.

This system enhances security by using Biometric authentication. Biometric equipment has the capability to measure, modify, compare, store, transmit and/or recognize a specific characteristic of a person with a high level of precision and trustworthiness. Biometric technology is based on the scientific fact that there are certain characteristics of living forms that are unique and not repetitive for each individual; these characteristics represent the only technically viable alternative to positively identify a person without the use of other forms of identification more susceptible to fraudulent behaviour. There are two major categories of biometric techniques: physiological (fingerprint verification, iris analysis, hand geometry-vein patterns, ear recognition, odour detection, DNA pattern analysis and sweat pores analysis) and behavioural (handwritten signature verification, key stroke analysis and speech analysis).

Fingerprints are distinctive and persistent. Everyone has different fingerprints which do not change over a lifetime. Fingerprint solutions offer many advantages which address the human factors of authentication and it has the following distinct features:

- One-of-a-kind identifiers: Fingerprints from each one of our ten fingers is distinctive, different from one another and from those of other persons.

- Relatively equal security level for all users in a system-one account is not easier to break into than any other (such as easily guessed password or through social engineering).
- Ensures the user is present at the point and tie of recognition and later cannot deny having accessed the system.
- Cannot be shared, lost, stolen, copied, distributed or forgotten unlike passwords, PINs and smart cards. Fingerprints strongly link an identity to a physical human being making it difficult for attackers to forge.
- Long history of successful use in identification tasks.

CHAPTER-2

LITERATURE REVIEW

The purpose of a literature review is to, provide foundation of knowledge on topic, identify areas of prior scholarship to prevent duplication and give credit to other researchers, identify inconstancies: gaps in research, conflicts in previous studies, open questions left from other research, identify the relationship of works in context of its contribution to the topic and to other works, place our own research within the context of existing literature making a case for why further study is needed.

Title of the paper	Year of Publication	Method Proposed	Limitations
OTP Based Card-Less Transaction using ATM [1]	2019	Unique number named BPIN which consists of a 6-digit Bank Identification Number (BIN), a 4-digit Personal Identification Number (PIN) and OTP is used.	There is no fingerprint-based approach for theft detection.
Authentication of Biometri System using Fingerprint Recognition with Euclidear Distance and Neural Network Classifier [2]	2019	Image acquisition and pre-processing for fingerprint verification algorithms.	No two-level security proposed in the system, reason being the absence of usage of OTP technology.
Security and Accuracy of Fingerprint based Biometrics: A Review [3]	2019	Eight possible attack points to a typical biometric authentication system.	The user must pay extra charges when he/she transacts from multiple accounts.
Enhanced ATM Security System using GSM GPS and Biometrics [4]	2019	8 ways of fraudulent transactions that can occur in the ATM system.	Comparisons with existing approaches show comparable performance to traditional approaches using BCS and CB techniques.
New Distribution Channels in Banking Services [5]	2018	Law enforcement agencies are responsible to enforce laws in fraud cases.	The user must remember PINs for all the ATM cards that he has.

Highly secure multiple account bank affinity Card-A successor for ATM card [6]	2018	Arduino Mega, RFID tag, RF Reader, RS232, Fingerprint scanner is used for the smart ATM card transaction.	Materials like metal and liquid can impact the signal when there is usage of RFID tags.
Prevention of ATM Robbery Using Advance Security [7]	2018	Usage of fingerprint as a biometric to prevent ATM robbery.	The main drawback is the false rejection of users when a fingerprint scanner is used.
ATM for visually challenged people. [8]	2017	Assisting visually impaired people to access the ATM system with RSA algorithm implementation to encrypt and decrypt.	Requires user training in order for them to operate the system.
Fingerprint Based Biometric ATM Authentication System [9]	2017	Biometric Cryptosystem for VoIP Security using Key Generation technique.	The newly proposed approach involves key extraction, which is a resource consuming task.

Table 2.1: Literature Review

CHAPTER-3

SCOPE / OBJECTIVES

The motivation of this process is to make an attempt to resolve the limitation observed in the existing system or security in the Automated Teller Machine (ATM). The proposed project is set out to create a Remote Authorization using a time-based OTP and fingerprint scan, so as to create a two-stage verification. The project aims to counter certain other small issues that exist in practice now. The existing technology uses a less secure 4-digit PIN and has a single stage verification. There's also an added drawback of a card being limited to a single bank account.

Currently a team at an organisation has proposed a Remote Authorization that requires ATM scanners to be included in every ATM. This would cost a lot of overhead to the authorities in terms of acquiring scanners and installing it in large number of ATMs. The proposed project comes up with an idea that uses a unique time-based OTP and also gives an option of fingerprint scan. The smart card that we provide can be linked to multiple accounts. A dedicated android application and a server will be set up to facilitate smooth transactions.

CHAPTER-4

CHALLENGES AND MOTIVATION

Presently, of the most modern ATMs, the ATM card used by the customer for each bank account which is a plastic ATM card with a magnetic stripe or a plastic smart card with a chip. However, password PIN which is the main authentication for ATM transactions represent the weakest link in the computer security chain. ATM services are popular because of their easiness for banking systems. In modern ATMs, the customer account can be identified by inserting a plastic card with magnetic strip that contains account number. The customer then verifies identity by entering a pass code i.e., personal identification number

(PIN) of four digits. The drawbacks of the existing systems are: -

- User must carry more ATM cards for more bank accounts.
- There is no OTP based technology with two level verification.
- When transaction is done from different ATMs user has to pay extra charges.
- User must remember PINs for all ATM cards.
- There is no fingerprint and theft detection.
- PIN is the weakest link in the existing system.
- Due to the moisture depositing on the keyboard hackers can easily access the password and there is no highly secured system.

CHAPTER-5

METHODOLOGY

The methodologies implemented in the project to build a 2-stage biometric verification for ATM Transactions are:

5.1 ATM

The ATMs are networked and connected to a centralized computer (Switch), which controls the ATMs. The use of biometric identification is possible at an ATM. The information can be stored at a bank branch or Network Provider. The typical ATM has two input devices (a card reader and keypad) and four output devices (display screen, cash dispenser, receipt printer, and speaker). Invisible to the client is a communications mechanism that links the ATM directly to an ATM host network.

The ATM functions much like a PC, it comes with an operating system (usually OS/2) and application software for the user interface and communications. While most ATMs use magnetic strip cards and personal identification numbers (PINs) to identify account holders, other systems may use smart cards with fingerprint validation.

5.2 PIN

The ATM forward information read from the client's card and the client's request to a host processor, which routes the request to the concerned financial institution. If the cardholder is requesting cash, the host processor signals from the customer's bank account to the host processor's account. Once the funds have been transferred, the ATM receives an approval code authorizing it to dispense cash.

If the number is entered incorrectly several times, usually the most ATMs will retain the card as security precaution to prevent an authorized user from assuming the PIN by guesswork and so on. Moreover the customer has to pay transaction fees. By keeping all burdens aside, a novel approach bank affinity card been proposed in this project.

5.3 Fingerprint

The host systems can reside at a client's institution or be part of an EFT network. The EFT network supports the fingerprint authentication with the fingerprint reorganization method we also embedded the GSM technique. If the fingerprint in the database matches the system will allow the user to perform further transactions. Fingerprint options cannot be simply duplicated which suggests solely the licensed person gets access and that we get high level of security. Factors such a generality, uniqueness, permanence, collectability, acceptableness, escape, performance should be applied for suitableness of attribute in biometric identification. It'ssignificantly predominant to secure and evidence data in an intelligent system. It cannot be shared, taken, and formation is not possible much in a very biometric system.

- A Smart RFID/NFC card is provided to the customer which is used to start the transaction.
- The Server on receiving the ATM transaction request sends a notification to the client's phone using Firebase Cloud Messaging.
- On clicking the push-message the app in the client side is launched to verify the transaction.
- The Server and client use TOTP library to generate one-time passwords.
- The client selects the bank account for the current transaction.
- Once the smartphone authenticates the client's fingerprint the OTP is encrypted on the client's device and sent to the server.
- The Server then authorizes the ATM transaction.

5.4 Raspberry Pi 3:

It is used to build a mock-up ATM to test the functionality of our project, it interfaces with the RFID receiver to start transactions.

Specifications:

The Raspberry Pi 3 Model B is the earliest model of the third-generation Raspberry Pi. It replaced the Raspberry Pi 2 Model B in February 2016.The latest product in the Raspberry Pi 3 range.

- Quad Core 1.2GHz Broadcom BCM2837 64bit CPU
- 1GB RAM

- BCM43438 wireless LAN and Bluetooth Low Energy (BLE) on board
- 100 Base Ethernet
- 40-pin extended GPIO
- 4 USB 2 ports
- 4 Pole stereo output and composite video port
- Full size HDMI
- CSI camera port for connecting a Raspberry Pi camera
- DSI display port for connecting a Raspberry Pi touchscreen display
- Micro SD port for loading your operating system and storing data

Fig-5.1: Rasberry Pi3

- Upgraded switched Micro USB power source up to 2.5A

5.5 Python WebSocket Server:

It is used to establish a full-duplex connection between client and server over a single TCP connection. A WebSocket connection allows full-duplex communication between a client and server so that either side can push data to the other through an established connection. The reason why WebSocket's, along with the related technologies of Server-sent Events (SSE) and WebRTC data channels, are important is that HTTP is not meant for keeping open a connection for the server to frequently push data to a web browser.

5.6 Redis:

Redis is an open source (BSD licensed), in-memory data structure store, used as a database, cache, and message broker. Redis provides data structures such as strings, hashes, lists, sets, sorted sets with range queries, bitmaps, hyperloglogs, geospatial indexes, and streams. Redis has built-in replication, Lua scripting, LRU eviction, transactions, and different levels of on-disk persistence, and provides high availability via Redis Sentinel and automatic partitioning with Redis Cluster. It is used in-memory database is used to map the transaction with the client device.

5.7 FireBase Cloud Messaging:

- Firebase Cloud Messaging (FCM) is a cross-platform messaging solution that lets you reliably send messages at no cost.
- Using FCM, you can notify a client app that new email or other data is available to sync. You can send notification messages to drive user re-engagement and retention. For use cases such as instant messaging, a message can transfer a payload of up to 4KB to a client app. It is used to dispatch push notification to client devices.

5.8 PyAuth library(python):

PyAuth is a two-factor authentication program compatible with Google Authenticator and other software and hardware using the standard TOTP algorithm outlined in RFC 6238 (support for the HOTP algorithm outlined in RFC 4226 is planned).Secrets are encrypted using AES256, there is no option for storing unencrypted secrets. If you were using an older beta version, you will be prompted for a password and the stored secrets will be migrated to the current encryption without requiring any more user intervention. It generates TOTP at the server and also verifies TOTP generated by the client.

5.9 RFID Card Reader (SL500)

Being developed based on NXP RFID technology, SL500 series desktop reader/writer are classified into SL500L, SL500A, SL500D and SL500F four types, the below sheet shows its category and price message. These proximity readers support ISO14443A, ISO14443B and ISO15693 passive cards, tags

Fig-5.2: RFID Card Reader (SL500)

and labels. Free SDK is provided, it helps an engineer to programming his/her own applications. The package is composed of PC_DEMO software, WinAPI and prototype description, USB driver, sample source code in C#, VC, BC, VB, PB and DELPHI.

5.9.1 RFID Cards

The easiest way to clone Mifare NFC Classic 1K Cards is by using an Android smartphone with NFC capabilities. That's right, your cell phone can be used to compromise the security of a company if they are using these types of cards (RFID security system).

Just download the "Mifare Classic Tool" for Android, but of course you need to turn on NFC. Go to your settings and search for NFC, make sure to enable it. Cloning cards that have never changed their default sector password.

5.10 Crypto library(dart):

It generates TOTP at the client side.

5.11 Pycryptodome:

PyCryptodome is a self-contained Python package of low-level cryptographic primitives.

PyCryptodome is a fork of PyCrypto. It brings several enhancements with respect to the last official version of PyCrypto (2.6.1), for instance: Authenticated encryption modes (GCM, CCM, EAX, SIV, OCB) Accelerated AES on Intel platforms via AES-NIFirst class support for PyPyElliptic curves cryptography (NIST P-256, P-384 and P-521 curves only).

Better and more compact API (nonce and iv attributes for ciphers, automatic generation of random nonces and IVs, simplified CTR cipher mode, and more)SHA-3 (including SHAKE XOFs) and BLAKE2 hash algorithms,Salsa20 and ChaCha20 stream ciphers scrypt and HKDF Deterministic (EC)DSA Password-protected PKCS#8 key containers Shamir's Secret Sharing scheme Random numbers get sourced directly from the OS (and not from a CSPRNG in user space) Simplified install process, including better support for Windows, Cleaner RSA and DSA key generation (largely based on FIPS 186-4),Major clean ups and simplification of the code base.It is used for encryption and decryption of messages between client and server.

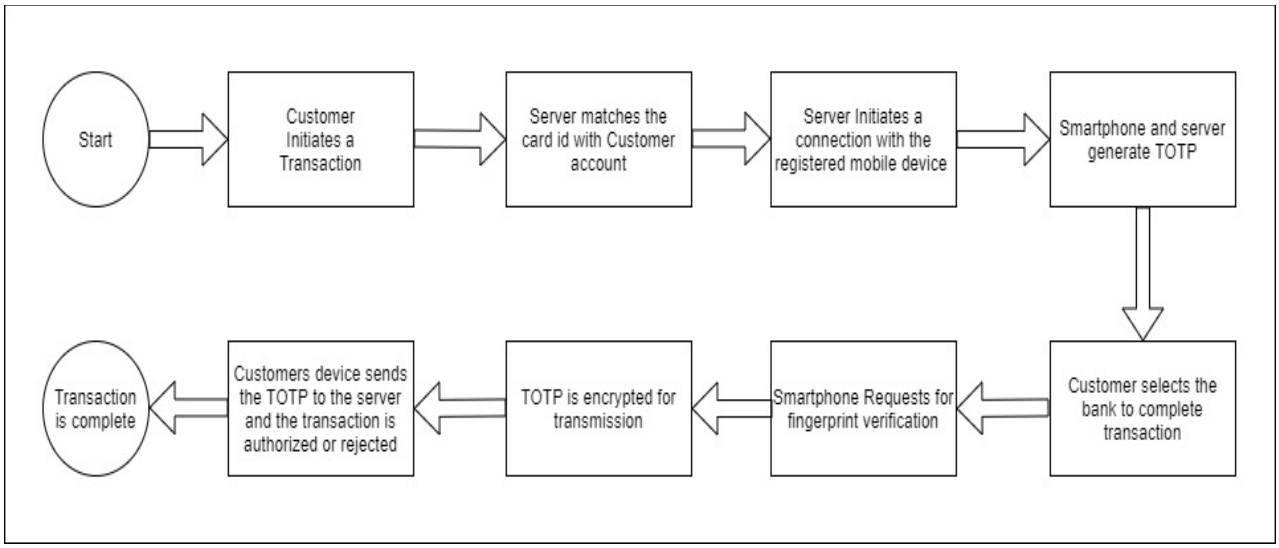

Fig-5.11: The flow of operations that takes place at each stage.

5.12 COMPARISION WITH EXISTING TECHNOLOGY

EXISTING TECHNOLOGY	OUR IMPLEMENTATION
Uses a less secure 4-digit PIN.	Uses a unique time-based OTP.
Single stage verification.	Gives an option of fingerprint scan.
A card can only be linked to a single bank account.	The smartcard can be linked to all of the user's accounts.
The existing proposal requires every ATM to include fingerprint scanners.	A dedicated application and a server are set up to facilitate transactions.

Table -5.12: COMPARISION WITH EXISTING TECHNOLOGY

CHAPTER-6

EXPECTED OUTCOME OF THE PROJECT

The Personal Verification Number (PIN) alone does not provide security. As fingerprints of every individual is unique and can be used for authentication, this system combines the pin verification and fingerprint recognition technology for identification. Along with fingerprint recognition technology and pin verification the GSM modem connected to the microcontroller generates the four-digit one-time password and sends to the main user mobile number when the user opts for OTP as a part of authentication. The fingerprint of the card holder is collected and stored in the database.

Every fingerprint of authenticated user is checked by the database. The four-digit one-time password should be entered by pressing the keys on the touch screen. After entering all the correct information customer can begin the further transaction. The biometric features cannot be replicated, this system will go a long way to solve the problem of account safety.

CHAPTER-7

REFERENCES

[1] www.flutter.dev/

[2] https://pycryptodome.readthedocs.io/en/latest/src/cipher/aes.html

[3] https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

[4] dev.mysql.com › doc

[5] www.raspberrypi.org › documentation

[6] https://www.cse.wustl.edu/~jain/cse574-06/ftp/rfid/index.html

[7] SBI implementation of OTP based system to withdraw amount above 10K

[8] Flutter for Beginners: An introductory guide to building cross-platform mobile applications

[9] Flutter and Dart 2 Paperback – Import, 12 September 2019

[10] Python Made Easy: Step by Step Guide to Programming and Data Analysis using Python for Beginners and Intermediate Level