

# Mobile Assisted Modified ATM for Visually Challenged

Dr L. M. Varalakshmi 1<sup>st</sup>  
Department of ECE  
Sri Manakula Vinayagar Engineering College,  
Puducherry, India.  
E-mail: varalakshmi@smvec.ac.in

R.Kurinjimalar  
Department of ECE  
Sri Manakula Vinayagar Engineering College  
Puducherry, India.  
E-mail: kurinji810@smvec.ac.in

**Abstract:** This project focuses on the way to enhance the features of the present working ATMs. This project can be divided into three modules. First module works to detect the arrival of the visually challenged person at the door and activates the special modules which is installed inside the ATM centre. This detection is made possible by the RFID technology. Once, the arrival of the visually challenged person is confirmed at the door, an instructing voice navigates the blind person towards the ATM machine. Then the mobile phone is used thereafter to give voice commands to the ATM machine for the transaction process. Again the instructing voice navigates the person towards the door carefully.

**Keywords:** ATM security, authentication, RFID, GSM , Module

## I. INTRODUCTION

In this work, the modified features of the ATM for visually challenged people are security and authentication using the mobile app and transaction process using the voice recognition facility. These features are implemented using the Raspberry Pi processor, Arduino UNO controller, RFID scanner, speakers and GSM module. This project helps the visually challenged people in using the normal ATMs by adding some extra features to it. An RFID tag with all the user's information is used to identify the user. A mobile app is created for giving commands to the ATM for each of its option window. A GSM module is used for authentication process by sending OTP.

The identification process is by using the RFID. When the person enters into the ATM, the RFID tag will be scan by the RFID scanner, which is present in the mobile backside and will send the message to the mobile number that is store in the RFID tag. The message will contain WIFI password and the OTP. The password will be used to connect the WIFI to the ATM hotspot. The OTP will be for the transaction process.

The authentication and security of the transaction processes are ensured. For authentication, an OTP is sent to the user's number by GSM module. For security purposes, a fingerprint lock is needed to access the speech recognition page of the mobile app.

The transaction process is done by using the mobile app and ATM. The ATM and mobile app will interface there by transaction process will takes place. The blind person will speak to the designed mobile app and the ATM will respond to

the mobile app and there by transaction process takes place either the withdrawal or balance check

## II. IDENTIFICATION

In this module of the project, the user (visually challenged people) is identified. His details like account number, phone number and his account's balance are inferred. This inferring is possible by scanning the RFID tag stick to the mobile's back by a RFID scanner.

### A. RFID Tag

**Radio-frequency identification (RFID)** uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically-stored information. Passive tags collect energy from a nearby RFID reader's interrogating radio waves. Active tags have a local power source (such as a battery) and may operate hundreds of meters from the RFID reader. Unlike a barcode, the tag need not be within the line of sight of the reader, so it may be embedded in the tracked object. RFID is one method for Automatic Identification and Data Capture (AIDC).

RFID tags are used in many industries, for example, an RFID tag attached to an automobile during production can be used to track its progress through the assembly line; RFID-tagged pharmaceuticals can be tracked through warehouses; and implanting RFID microchips in livestock and pets allows for positive identification of animals.

### B. RFID Reader

An RFID reader transmits an encoded radio signal to interrogate the tag. The RFID tag receives the message and

then responds with its identification and other information. This may be only a unique tag serial number, or may be product-related information such as a stock number, lot or batch number, production date, or other specific information. Since tags have individual serial numbers, the RFID system design can discriminate among several tags that might be within the range of the RFID reader and read them simultaneously.

RFID systems can be classified by the type of tag and reader. A Passive Reader Active Tag (PRAT) system has a passive reader which only receives radio signals from active tags (battery operated, transmit only). The reception range of a PRAT system reader can be adjusted from 1–2,000 feet (0–600 m), allowing flexibility in applications such as asset protection and supervision.

An Active Reader Passive Tag (ARPT) system has an active reader, which transmits interrogator signals and also receives authentication replies from passive tags. An Active Reader Active Tag (ARAT) system uses active tags awoken with an interrogator signal from the active reader. A variation of this system could also use a Battery-Assisted Passive (BAP) tag which acts like a passive tag but has a small battery to power the tag's return reporting signal.

### III. AUTHENTICATION

In this module the authentication and security of the transaction processes are ensured. For authentication, an OTP is sent to the user's number by GSM module. For security purposes, a fingerprint lock is needed to access the speech recognition page of the mobile app.

#### A. Global System for Mobile communication(GSM)

GSM (Global System for Mobile Communications), is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation digital cellular networks used by mobile devices such as tablets, first deployed in Finland in December 1991. As of 2014, it has become the global standard for mobile communications – with over 90% market share, operating in over 193 countries and territories.

Subsequently, the 3GPP developed third-generation (3G) UMTS standards, followed by fourth-generation (4G) LTE Advanced standards, which do not form part of the ETSI GSM standard. "GSM" is a trademark owned by the GSM Association. It may also refer to the (initially) most common voice codec used, Full Rate. The salient features of LM35 are:

#### GSM Module

##### B. Subscriber Identity Module (SIM)

One of the key features of GSM is the Subscriber Identity Module, commonly known as a SIM card. The SIM is a detachable smart card containing the user's subscription information and phone book. This allows the user to retain his or her information after switching handsets. Alternatively, the user can also change operators while retaining the handset simply by changing the SIM. Some operators will block this by allowing the phone to use only a single SIM, or only a SIM issued by them; this practice is known as SIM locking.

##### C. One Time Password (OTP)

A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also incorporate two factor authentications by ensuring that the one-time password requires access to something a person has (such as a small keying fob device with the OTP calculator built into it, or a smartcard or specific cell phone) as well as something a person knows (such as a PIN).

The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage is that a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further.

### IV. SECURITY

#### A. Fingerprint Matching

This module ensures the security of the whole system. Only when authorised user uses the app the speech recognition page will be accessed.

#### B. Fingerprint Sensor

Finger Print Sensor (R305) -TTL UART is a finger print sensor module with TTL UART interface. The user can store

the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the person. The finger print module can directly interface with 3v3 or 5v Microcontroller. A level converter (like MAX232) is required for interfacing with PC.

A fingerprint consists of ridges and valleys. They together provide friction for the skin. The main identification of the skin is based upon the minutiae, which actually is the location and direction of the ridge endings and splits along a ridge path.

There are mainly two types of scanning methods for this technology. Either an optical or capacitance scanner is used to scan and make a picture of your finger. Though both the methods produce the same type of image, the making of it is completely different.

## V. TRANSACTION PROCESS

In this module of the project, the visually challenged person responds to the each of the ATM's menu by giving appropriate voice commands via his mobile which is connected to the ATM.

### A. Speech Recognition

Speech recognition is the inter-disciplinary sub-field of computational linguistics that develops methodologies and technologies that enables the recognition and translation of spoken language into text by computers. It is also known as "automatic speech recognition" (ASR), "computer speech recognition", or just "speech to text" (STT). It incorporates knowledge and research in the linguistics, computer science, and electrical engineering fields.

Some speech recognition systems require "training" (also called "enrolment") where an individual speaker reads text or isolated vocabulary into the system. The system analyses the person's specific voice and uses it to fine-tune the recognition of that person's speech, resulting in increased accuracy. Systems that do not use training are called "speaker independent" systems. Systems that use training are called "speaker dependent".

### B. Wi-Fi Hotspot Connection

A hotspot is a physical location where people may obtain Internet access, typically using Wi-Fi technology, via a wireless local area network (WLAN) using a router connected to an internet service provider.

Public hotspots may be created by a business for use by customers, such as coffee shops or hotels. Public hotspots are typically created from wireless access points configured to provide Internet access, controlled to some degree by the venue. In its simplest form, venues that have broadband Internet access can create public wireless access by configuring an access point (AP), in conjunction with a router

and connecting the AP to the Internet connection. A single wireless router combining these functions may suffice. Here in this project a Hotspot has been provided in the ATM centre to which the ATM and the mobile phone of the user should be connected.

### C. Raspberry Pi

The Raspberry Pi is a series of small single-board computers developed in the United Kingdom by the Raspberry Pi Foundation to promote the teaching of basic computer science in schools and in developing countries. The original model became far more popular than anticipated, selling outside its target market for uses such as robotics. It does not include peripherals (such as keyboards, mice and cases). However, some accessories have been included in several official and unofficial bundles.

The Pi zero w versions processor speed ranges from 700 MHz to 1.4 GHz for the Pi 3; on-board memory ranges from 256 MB to 1 GB RAM. Secure Digital (SD) cards are used to store the operating system and program memory in either SDHC or MicroSDHC sizes. The boards have one to four USB ports. For video output, HDMI and composite video are supported, with a standard 3.5 mm phone jack for audio output. Lower-level output is provided by a number of GPIO pins which support common protocols like I<sup>2</sup>C. The B-models have an 8P8C Ethernet port and the Pi 3 and Pi Zero W have on-board Wi-Fi 802.11n and Bluetooth.

### D Arduino UNO

Arduino is an open source computer hardware and software company, project, and user community that designs and manufactures single-board microcontrollers and microcontroller kits for building digital devices and interactive objects that can sense and control objects in the physical and digital world. The project's products are distributed as open-source hardware and software, which are licensed under the GNU Lesser General Public License (LGPL) or the GNU General Public License (GPL), permitting the manufacture of Arduino boards and software distribution by anyone. Arduino boards are available commercially in preassembled form, or as do-it-yourself (DIY) kits.

Arduino board designs use a variety of microprocessors and controllers. The boards are equipped with sets of digital and analog input/output (I/O) pins that may be interfaced to various expansion boards or Breadboards (shields) and other circuits. The boards feature serial communications interfaces, including Universal Serial Bus (USB) on some models, which are also used for loading programs from personal computers.

The microcontrollers are typically programmed using a dialect of features from the programming languages C and C++. In addition to using traditional compiler tool chains, the Arduino project provides an integrated development environment (IDE) based on the Processing language project.

## VI. PROPOSED WORK

This project focuses on the way to enhance the features of the present working ATMs. This project can be divided into three modules.

First module works to detect the arrival of the visually challenged person at the door and activates the special modules which are installed inside the ATM centre. This detection is made possible by the RFID technology.

Once, the arrival of the visually challenged person is confirmed at the door, an OTP and Wi-Fi password is sent via the GSM.

Then the mobile phone is used thereafter to give voice commands to the ATM machine for the transaction process. The Arduino UNO board controls the GSM, IR Sensor and RFID reader.

Raspberry Pi zero connected to hotspot and speaker. The ATM menus are asked by the speaker and the responses are received from the mobile app. This mobile phone and Pi are connected to the same hotspot. The block diagram of this project is shown in Fig. 1

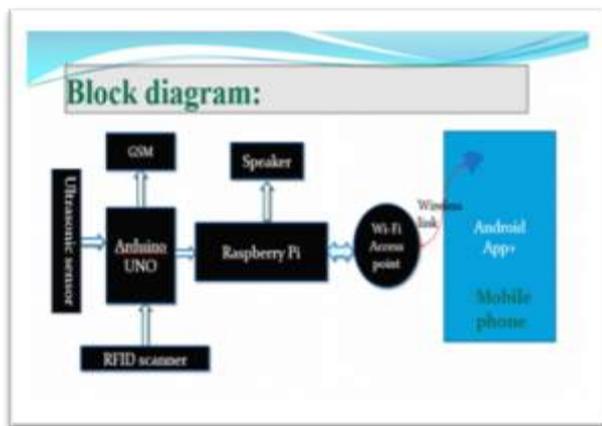


Fig 1. Block Diagram of Proposed work

## VII. INTERFACING

The GSM 900A module's transmitter and receiver pins are connected to the pin 10 and 11 of the Arduino UNO board. These pins are enabled by software serial. The +12 volt power supply to the GSM is given via the 12V adapter. Arduino

board is supplied with power by 9V adapter. RFID reader's Tx pin is connected to the Rx pin of Arduino board. RFID reader is supplied with +5V from Arduino board. IR sensor is connected to the pin 7 of the Arduino board. This sensor is supplied with +5v from Arduino board. From pin 5 to GPIO 10 of Raspberry Pi Zero. ( Fig. 2)

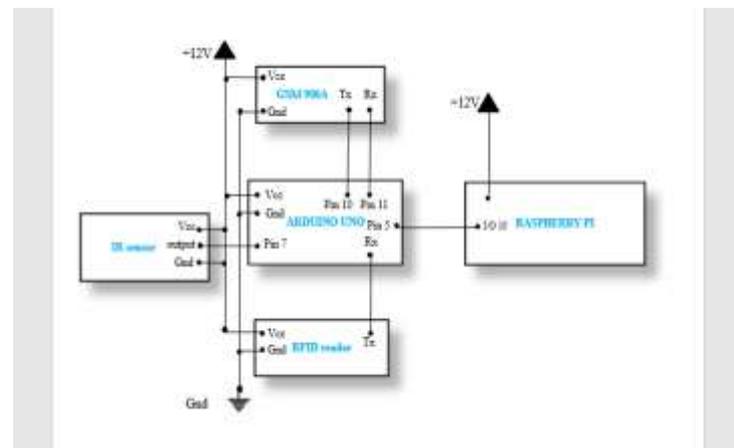


Fig. 2 Interfacing of the proposed work

## VIII. CONCLUSION

Initially the users account details are fed in the app while doing the registration at the bank. The RFID is given to the user. While entering the ATM, at the door level scanning of the RFID is done. So that information like account number, mobile number of the user and the bank statement is collected. Then the mobile APP is turned on, the mobile APP automatically connects to the ATM Wi-Fi and the connections between the interface are made. Then the voice commands are given by the user, the commands are received by the ATM and the transactions are done.

## REFERENCES

- [1] Ashish M. Jaiswal, Mahip Bartere, "Enhancing ATM Security using Fingerprint and GSM technology", International Journal of Computer Science and Mobile Computing, Vol: 3, Issue: 4, April -2014, pg. 28-32.
- [2] Guruprasad.S.S, I. Nagarathna, Nandini.B, Roja.K.S, "Smart ATM Supervision System using GSM", International Journal of Research and Scientific Innovation, Vol: IV, Issue: VI, June 2017.

- [3] Sasirekha K, Nivetha M, Indhumathi A, Renukadevi D, “ATM machine for Blind people”, International journal of chemical science 14(S3), 2016, pg.911-916.
- [4] Ahmed Farooq, “Haptics in ATMs & Kiosks”, University of Tampere, Department of Computer Sciences, Raisamo, December 2008.
- [5] Okebiro Jared Omarai, Omariba Bosire Zacharya, “Investigating ATM system accessibility for people with visual impairments”, IOSR Journal of Computer Engineering (IOSR-JCE), Vol 15, Issue 5 (Nov- Dec 2013), PP13-18.

### AUTHOR’S BIOGRAPHIES



Dr. L. M. Varalakshmi is currently working as Professor in the Department of Electronics and Communication Engineering at Sri Manakula Vinayagar Engineering college affiliated to Pondicherry University, Puducherry, India. She has completed her B.E. in Electronics and Communication Engineering from

Thiagarajar College of Engineering, Madurai and M.Tech. in Electronics and Communication Engineering from Pondicherry Engineering College, Puducherry. She has more than 20 years of teaching experience. Her Research interests include Cryptography and Multimedia security. She has published more than 30 papers in various journals.



R. Kurinjimalar received B.E degree in Electronics and Communication Engineering from Bharathidasan University, Trichy, Tamilnadu, India in 1997 and her M.E degree in Communication Engineering from Vinayaga Mission University,

Salem, India in 2007. She has Eighteen years of teaching experience. She is currently working as Associate Professor in the Department of Electronics and Communication Engineering at Sri Manakula Vinayagar Engineering College affiliated to Pondicherry University, Pondicherry, India. She is a part time Research Scholar in the Department of Electronics and Communication Engineering, SCSVMV University, Enathur, Kanchipuram, India. She has published 19 papers in International Journals and proceedings of IEEE International Conferences, including the publication listed in this thesis. Her research interests include mobile satellite networks and wireless communication.