JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

PERSONALISED ATM PIN GENERATING SYSTEM

Dr.S.M. Swamynathan[01], B. Manikandan[02], B.R. Kannaka Subbu Lakshmi[03], G. Bhavithra[04], S. Arunagirinathan[05]
UG Scholar, B.E. Electronics and Communication Engineering
[01]SNS College of Technology

ABSTRACT: - An automated teller machine (ATM), also called a cash machine in British English, is a type of electronic telecommunications tool that allows users to conduct financial transactions, such as cash withdrawals, deposits, funds transfers and balance inquiries whenever they want and without having to speak with bank employees directly. On June 27, 1967, Barclays Bank put in the first ATM in Enfield Town, London. Other names for ATMs include Automated Banking Machine, Cash Point (in Britain), Hole in the Wall, Ban Comet (in Europe and Russia), and Any Time Money (in India). Theft from ATMs has significantly increased in recent years, and this includes shoulder attacks that record pin numbers. This technology is employed in pin entry access systems to stop ATM shoulder attacks. The majority of PIN entry methods are susceptible to observational attacks. To strengthen defenses against observational attacks, a haptic feedback device was employed. In order to access the ATM, the user then calculates his pin (personal pin plus randomly generated pin) and enters the newly created pin. If the user inputs the wrong pin, a message will appear on the registered mobile device requesting them to confirm using the GPS module. We use temperature sensors for increased security because they generate random numbers as a result of their daily temperature performance. The suggested solution uses a vibrator and temperature, and its goal is to increase defense against observational attacks.

Keywords: Vibrator Motor, Temperature Sensor, GPS Module.

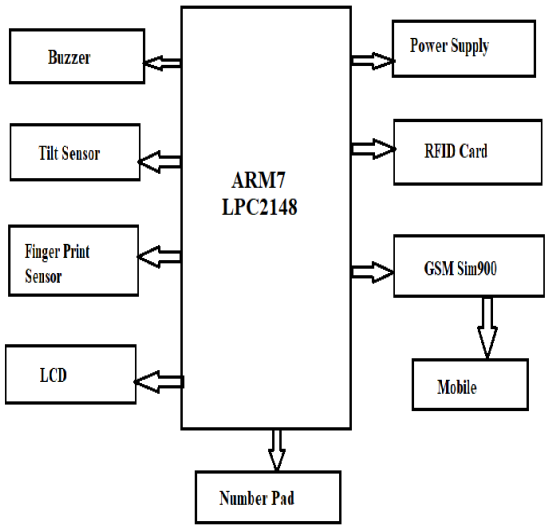
1. Introduction

Money can be deposited and withdrawn from an ATM. A card is inserted into an ATM processor, which is an automatic teller machine that exchanges money for the card. ATMs come in two different varieties. To dump money by the user and receive a receipt based on the account is the first type. The second kind is more sophisticated; it allows for credit card payments, cash deposits, and account information retrieval. Several people utilize ATMs to deposit cash. In order to make it simple to remember, an ATM machine that is close to the user's location can be used to obtain cash if that is what they need. According to user needs, an ATM machine has two inputs and four outputs. Each ATM card has a distinct number, known as a PIN number. If the card is recognized, the system will prompt the user to enter their PIN. If the PIN is entered correctly, the ATM will begin the transaction process; otherwise, it will be blocked. Each user has the option of changing their PIN number to one that is simple to remember. The output of the ATM machine includes a display screen, a receipt printer, a cash dispenser, and speakers. However, we offer Loc-HapPIN, a revolutionary PIN-entry system that is resistant to observation assaults and provides localized haptic feedback, for touchscreen

devices and keypads. The usability and resilience to surveillance attacks will be enhanced by the localized haptic feedback technology.

2. EXISTING TECHNIQUE: -

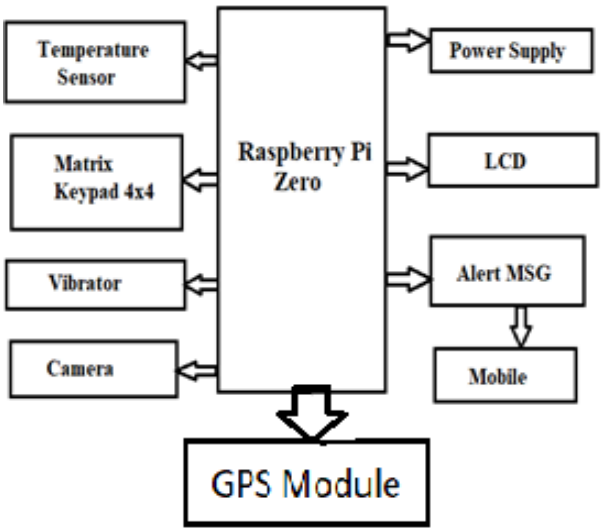
This existing technique propose a system of OTP and biometrics are being used in the proposed system to secure ATM user transactions.



Here, we utilize an RFID card as an ATM card, enter the amount and the OTP using the number pad, send the OTP through GPS to the registered mobile number, and use a fingerprint scanner for biometric security. The result of the entire system is presented on the LCD. In addition, a tilt sensor is utilized to increase the security of the ATM machine; if somebody attempts to take the device, there will be tilting, which is detected by a tilt sensor connected to the ATM machine and signaled by a buzzer alarm. The ARM7 LPC2148 microcontroller is connected to all these sensors.

3. Proposed System

To provide localized haptic feedback on touchscreen devices and keypads, we present Loc-HapPIN, a new observation attack-resistant PIN-entry system. The resistance to observation attacks and usefulness will both be enhanced using localized haptic feedback technologies. Observational attacks can exploit common PIN-entry methods. Some PIN-entry techniques for mobile devices based on audios and/or haptics that are resistant to observation attacks have been presented to increase such resistance. But none of the PIN-entry systems currently in use are both highly usable and impervious to observation assaults. In this article, we suggest Loc-HapPIN, a new PIN-entry system for touchscreen devices that may provide localized haptic feedback and is immune to observation assaults. It is possible to increase usefulness and resistance to observational attacks by utilizing localized haptic feedback technologies. The user can also select the efficiency-security configuration that is best for him. The proposed system's functions and the content that goes into them are depicted in a block diagram. Theft from ATMs has greatly escalated in recent years. By merging the card number and the password, or by seeing the password while inputting the pin using a webcam and saving the number while the card is being swiped, various thefts can be committed. Numerous strategies, including GPS with OTP, have been implemented to combat ATM theft. When using the OTP technique, a one-time password is simply sent to the user after their card is swiped at an ATM, allowing them to input it to access the transaction. The approach has several drawbacks, such as the possibility of a mobile device or signal issue, which would prevent the person from receiving the one-time password at that precise moment, or the possibility that they might forget to bring their phone to the ATM.



3.1 Working of Proposed System

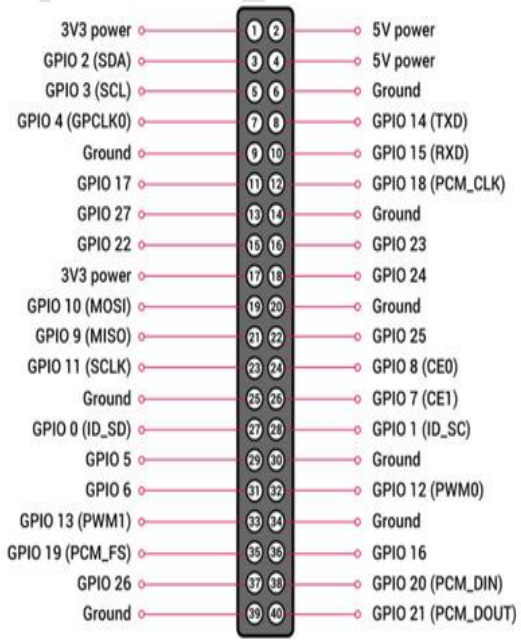
As a result, we are putting out a fresh approach that integrates haptic feedback to stop ATM theft. The vibrator that is employed in the ATM keypad is haptic in the strictest sense. The user must touch the keyboard to activate the haptic feedback technology after the card has been swiped to feel the vibration. If the person's pin is 1234, for instance, and the keypad vibrates three times, we must add that to the first pin number, which is one, to get four. If the keypad vibrates five times, for example, we must add that to the second pin number, which is two, to get seven. The original pin number must then be added to the received vibrations in this manner. The user password will be altered based on the vibrations when the Card is swiped, but the initial password will remain the same because the vibrations are generated randomly. We use temperature sensor for increased security because they generate random number because of their daily temperature performance.

For strengthening security, A notification asking the user to confirm using the Raspberry Pi Camera and GPS module will show up on the registered mobile device. If the user enters the incorrect pin the assailant was photographed using a Raspberry Pi camera, and the location of the ATM where the robbery took place was identified using a GPS module. And the notification is sent to nearby Police station. By this ATM theft can be decreased using this method because the individual can feel the vibrations, preventing them from being observed, and since the vibrations are generated at random each time, preventing ATM theft from happening any longer.

4. System Hardware

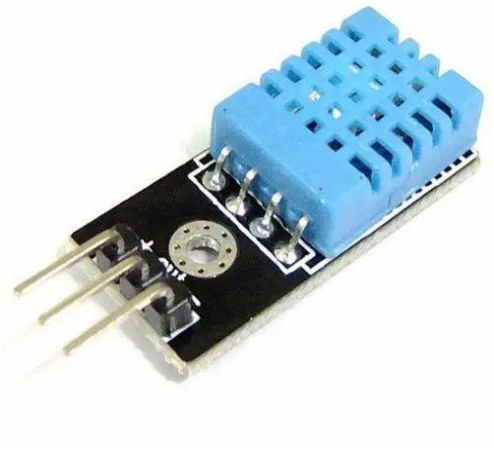
4.1. Raspberry Pi Zero

A computer with built-in Wi-Fi and Bluetooth, the Raspberry Pi Zero W is incredibly small, cheap, and hackable. The Raspberry Pi Zero is quicker than the Raspberry Pi 1 thanks to its BCM 2835 (32-bit ARM based processor) SoC running at 1GHz. Although you'll definitely need some accessories to help you connect it to your existing devices, it still offers excellent connection with mini-HDMI, micro-B OTG USB, and the same 40-pin GPIO. The nicest aspect of this is that the Pi Zero W retains the same dimensions, connections, and mounting holes as the Pi Zero v1.3. Except for cases with metal tops, 99% all cases and accessories will still be fully compatible with both the Pi Zero W and v1.3. The Zero W features Bluetooth 4.0 and 802.11n wireless LAN connectivity, just like the Raspberry PI 3. If a Bluetooth keyboard or mouse is used instead of a USB keyboard or mouse, this frees up many of the connections that would have been made over USB, including a Wi-Fi dongle and a USB keyboard and mouse. An integrated camera connection is present on all Zero W models and the Raspberry Pi Zero V1.3+. To attach the Raspberry Pi Camera module, use this. The connector, meanwhile, is different from the regular Pi and has a 22-pin 0.5mm connector. For the camera to be connected to the Pi Zero W, a separate cable is required.



4.2. Temperature Sensor

A temperature sensor is an electronic device that measures the temperature of its environment and converts the input data into electronic data to record, monitor or signal temperature changes. Here we use temperature sensor to increase security against observation attacks.



4.3. Vibrator Motor

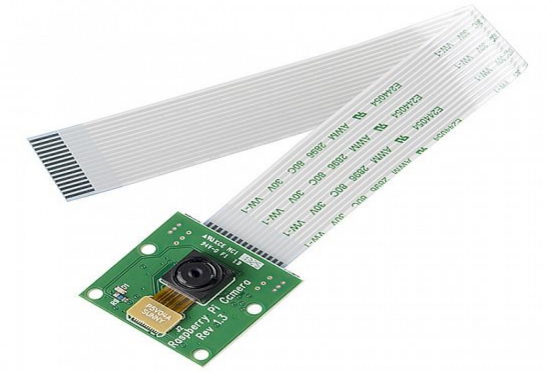
A vibration motor is an instrument that calculates the magnitude and frequency of vibration in a system, machine, or piece of machinery. Our input in this case came via a vibrator. To protect the user pin from shoulder strikes, the user randomly receives the vibration.

4.4. GPS Module

GPS modules contain tiny processors and antennas that directly receive data sent by satellites through dedicated RF frequencies. From there, it'll receive timestamps from each visible satellite, along with other pieces of data. Here we use a GPS Module to send location to user and nearby police station where ATM theft is occurring.

4.5. Camera

High resolution video and images can be captured using the Pi Camera module. The CSI (Camera Serial Port) interface on the Raspberry Pi Board allows us to directly connect the Pi Camera module to the board. Using a 15-pin ribbon cable, this Pi Camera module may be connected to the CSI port of the Raspberry Pi. Here, a camera is used to record the assailant as they attack the ATM.



Keypad

A group of keys in a printed circuit board is call keypad. And these keypads are used as input for ATM user for entering their pin.

5.Result

In the LCD, the outcome may be shown. The choice for ATM users is shown first.

The user has the option of checking their savings balance or withdrawing money.

The LCD shows that the user has successfully withdrawn a particular amount by inputting a valid password.

Using the GPS Module, a message alert is delivered to the user if they enter an invalid password, and it is displayed in the LCD here.

6.Conclusion

By employing these techniques, it is possible to improve defenses against observational attacks and lower ATM theft rates.

7.Reference

[1] ATM Shoulder – Security Resistant Pin Entry Using Based Pin and Base Text.
Mani Bharathi, Dhana Lakshmi and Raju2022, IEEE journal paper, June 6.

[2] ATM Shoulder – Surfing Resistant Pin Entry by Using Rand Word Generator. Prakasan Periasamy, Priya Dharshini, Saanthini and Sathya. ResearchGate journal, May 2019.

[3] ATM Pin Authentication Using Facial Recognition. Aishani Bangia and Prabu. Global Scientific Journal, October 2019.

[4] ATM Security Using Fingerprint Biometric Identifier: An Investigative Study.
Moses Okechukwu Onyesolu and Ignatius Majesty Ezeani.International Journal of Advanced Computer Science and Applications,2012.

[5] Usability and biometric verification at the ATM interface. Lynne Coventry, Antonella De Angeli and Graham Johnson. ACM Digital Libraries,2003.

[6] A Survey on Theft Prevention During ATM Transaction Without ATM Cards. Sistu Sudheer Kumar and A. Srinivas Reddy.International Journal of Research in Engineering and Technology,2015.