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

ATM PIN THEFT AVOIDANCE 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 known as a cash machine in British English, is a type of electronic telecommunications device that enables users to conduct financial transactions like cash withdrawals, deposits, funds transfers, and balance inquiries whenever they want and without having to speak with bank employees directly. The first ATM was installed by Barclays Bank on June 27, 1967, in Enfield Town, London. Additional 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 greatly grown recently, and this includes shoulder attacks that record pin digits. In pin entry access systems, this technology is used to prevent ATM shoulder attacks. The bulk of PIN entry techniques can be attacked using observational techniques. Using a haptic feedback device, defences against observational attacks were strengthened. The user then calculates his pin (his personal pin plus a randomly generated pin) and enters the brand-new pin to gain access to the ATM. If the user enters the incorrect pin, a message seeking confirmation using the GPS module will show up on the registered mobile device. Because temperature sensors produce random numbers as a result of their daily temperature performance, we use them for increased security. The proposed method increases defence against observational attacks by utilising a vibrator and temperature.

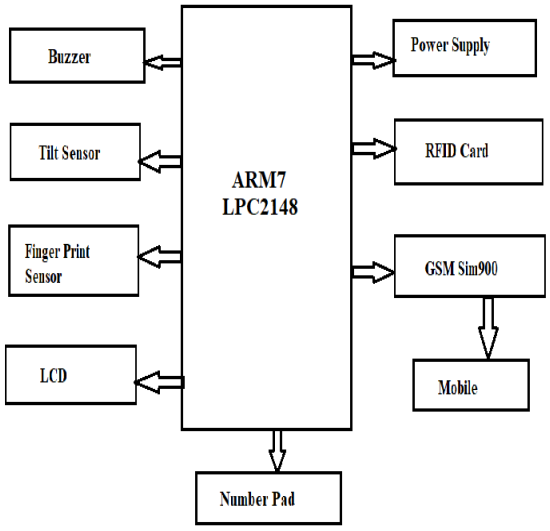
Keywords: *Vibrator Motor, Temperature Sensor, GPS Module.*

1. Introduction: -

An ATM allows for both deposits and withdrawals of cash. An ATM processor, also known as an automatic teller machine, accepts a card and exchanges money for it. There are two different types of ATMs. The first type allows the user to deposit money and receive a receipt depending on the account. The second type is more advanced and enables the use of credit cards, cash deposits, and account information retrieval. Many people use ATMs to make cash deposits. If the user needs cash, they can get it from an ATM machine close to their location, which will make it easy to remember. An ATM machine has two inputs and four outputs, depending on user needs. PIN numbers are unique numbers that are assigned to each ATM card. The user will be prompted to enter their PIN if the card is recognized by the system. The ATM will start the transaction procedure if the PIN is entered correctly; if not, it will be blocked. The PIN number for each user can be changed to one that is easier to remember. The output of the ATM machine consists of speakers, a display screen, a cash dispenser, and a receipt printer. But for touchscreen devices and keypads, we provide Loc-HapPIN, a ground-breaking PIN-entry system that is impervious to observational attacks and delivers localized haptic feedback. The localized haptic feedback technology will improve usability and resistance to surveillance attacks.

2. Existing Technique: -

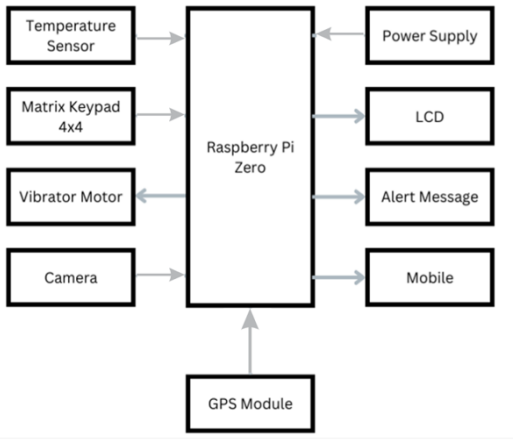
This method already in use proposes a system of OTP and biometrics are being employed in the proposed system to safeguard ATM user transactions.



Here, an RFID card is used as an ATM card, together with a number pad to enter the amount and the OTP, GPS technology to send the OTP to the registered cellphone number, and a fingerprint scanner for biometric security. On the LCD, the system's final output is displayed. Additionally, the ATM machine uses a tilt sensor to increase security. If someone tries to steal the device, there will be tilting, which is detected by a tilt sensor attached to the ATM machine and signaled by a buzzer alarm. All of these sensors are connected to the ARM7 LPC2148 microcontroller.

3. Proposed System

We introduce Loc-HapPIN, a new observation attack-resistant PIN-entry method, to deliver localized haptic feedback on touchscreen devices and keypads. The application of localized haptic feedback technology will increase both the resistance to observation attacks and usefulness. Common PIN-entry techniques can be exploited by observational attacks. To strengthen such resistance, some PIN-entry methods for mobile devices based on audios and/or haptics that resist surveillance attacks have been presented. However, none of the PIN entry systems in use today are both highly functional and resistant to observational attacks. In this work, we propose Loc-HapPIN, a novel touchscreen PIN entering system that may offer localised haptic feedback and is resistant to observational attacks. In this work, we propose Loc-HapPIN, a novel touchscreen PIN entering system that may offer localized haptic feedback and is resistant to observational attacks. Localized haptic feedback technology can be used to boost utility and resistance against observational attacks. The ideal efficiency-security setup for the user can also be chosen. A block diagram shows the functions of the suggested system and the data that goes into them. Recent years have seen a sharp increase in ATM theft. A number of thefts can be carried out by combining the card number and password, or by using a webcam to see the password while entering the pin and recording the number while the card is being swiped. To stop ATM theft, a variety of tactics have been used, including GPS with OTP. When a card is swiped at an ATM utilizing the OTP method, a one-time password is simply transmitted to the user, who must enter it to access the transaction. The method has a number of disadvantages, including the chance that a mobile device or signal issue would prevent the user from obtaining the one-time password at that specific moment or the likelihood that they would forget to bring their phone to the ATM.



3.1 Working of Proposed System

As a result, we are releasing a novel strategy that incorporates haptic feedback to prevent ATM theft. The ATM keypad uses a vibrator that is haptic in the purest sense. After the card has been swiped, the user must touch the keyboard to turn on the haptic feedback technology and experience the vibration. When the keypad vibrates three times when the user's pin, for example, is 1234, we must multiply the result by one to get four. For instance, if the keypad vibrates five times, we must multiply it by the second pin number of 2, which equals seven. Then, using this method, the received vibrations must be added to the original pin number. However, because the vibrations are generated randomly, the initial password will not change when the Card is swiped. Instead, the user password will be modified based on the vibrations. We utilize temperature sensors because they generate random numbers as a result of their daily temperature performance, which increases security.

TESTCASES

7890 – personal pin

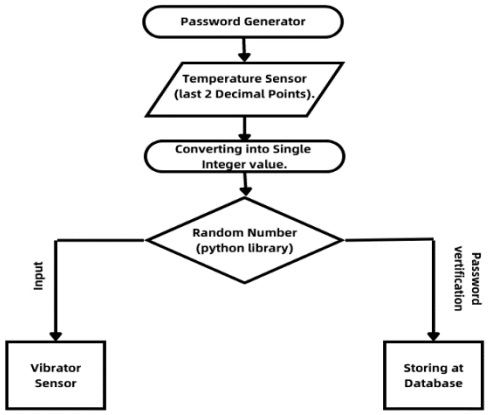
6532 – generated pin(enter)

3322 – generated pin(enter)

As a means of enhancing security, On the registered mobile device, a notification asking permission to use the Raspberry Pi Camera and GPS module will appear. If the user enters the wrong pin, a Raspberry Pi camera was used to capture the attacker, and a GPS module was used to pinpoint the location of the ATM where the robbery occurred. Additionally, the nearby Police station receives the notification. With this technique, ATM theft can be reduced because the person can feel the vibrations, preventing them from being observed, and because the vibrations are generated randomly each time, preventing ATM theft from happening any longer.

3.2 Flow Chart

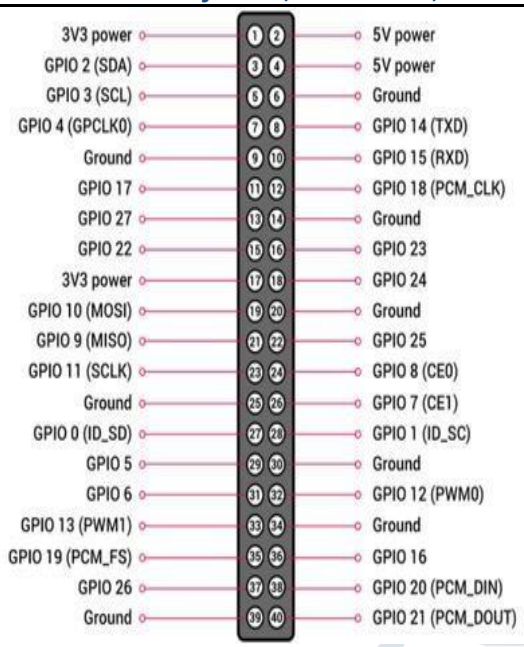
The flow chart describes how the password is generated to stop the theft of the ATM pin. A temperature sensor is used to generate the random number. The value is obtained in float form using the last two decimal places. Due to the random nature of decimal numbers, they are difficult to predict, making the process more secure. After that, a condition is used to convert the decimal to a single value. A Python library function that converts a decimal value into a single value is being used in this case. The value is processed using two techniques. That value is first used as the input for the vibrator sensor, and then we store the single integer in the database. The number is saved to see if the number on the keypad and in the database are same.



4. System Hardware

4.1 Raspberry Pi Zero

The Raspberry Pi Zero W is a wireless and Bluetooth-enabled computer that is very portable, reasonably priced, and hackable. Because of its 1GHz BCM 2835 (32-bit ARM based processor) SoC, the Raspberry Pi Zero is faster than the Raspberry Pi 1. It still offers good connection with mini-HDMI, micro-B OTG USB, and the same 40-pin GPIO, despite the fact that you'll undoubtedly need some adapters to assist you connect it to your existing devices. The Pi Zero W keeps the same size, connectors, and mounting holes as the Pi Zero v1.3, which is the finest feature of all. 99% of all cases and accessories, with the exception of those with metal tops, will still be fully compatible with both the Pi Zero W and v1.3. Many of the connections that would



have been made over USB, such as a Wi-Fi dongle and a USB keyboard and mouse, are freed up when a Bluetooth keyboard or mouse is used in place of a USB keyboard or mouse. On the Raspberry Pi Zero V1.3+ and all Zero W models, there is an integrated camera connection. Use this to affix the Raspberry Pi Camera module. The connector contains a 22-pin 0.5mm connector and is unique from the normal Pi. A different connection is needed to connect the camera to the Pi Zero W.

4.2 Temperature Sensor

In order to record, monitor, or communicate temperature changes, a temperature sensor is an electronic device that monitors the temperature of its surroundings and turns the input data into electronic data. Here, temperature sensors are used to boost defences against observational attacks.

4.3 Vibrator Motor

A vibration motor is a device that determines the strength and frequency of vibration in a machine, system, or piece of equipment. In this scenario, a vibrator was used as our input. The user randomly gets the vibration in order to shield the user pin from shoulder blows.

4.4 GPS Module

Dedicated RF frequencies are used by the GPS module's tiny processor and antennas to directly receive data from satellites. From each visible satellite, it will then obtain timestamps and other information. Here, we use a GPS module to transmit the location of the ATM theft to the user and a local police station.

4.5 Camera

The Pi Camera module allows for the capture of high-definition video and pictures. The Raspberry Pi Board's CSI (Camera Serial Port) interface enables us to directly attach the Pi Camera module to the board. This Pi Camera module can be attached to the Raspberry Pi's CSI port via a 15-pin ribbon cable. Here, the assault on the ATM is captured on camera by the assailant.

5. Result

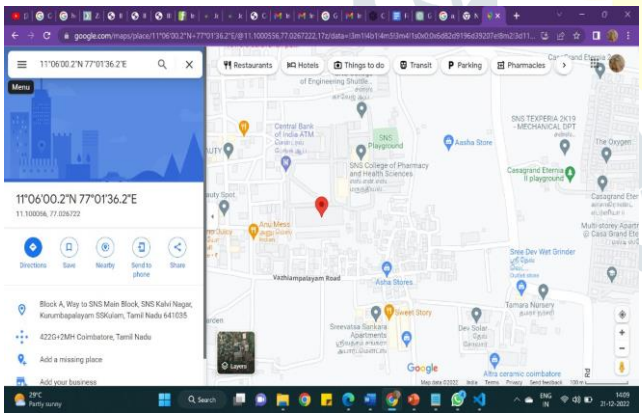
The result could be displayed on the LCD. The option shown to ATM users comes first.

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.

Message sent via the Twilio API.



Location of the ATM is sent to user via link using Twilio API.

6. Conclusion

By implementing certain strategies, it is plausible to strengthen the defences against observational assaults and reduce the occurrence of thefts at Automated Teller Machines (ATMs). These strategies can range from simple measures.

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. GlobalScientific 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 interfaces. 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.