ENHANCED SECURITY SYSTEM FOR ATM

Jigna Waghela , Mandar Shedge , Vishal Chikne , Dr. Pradip Mane
Dept of Information Tech
VPPCOE
Mumbai 400022, India

Abstract-
The customer can used this atm by 24/7. In this project we overcome the problem of atm pin hack and it is secure way to do transaction. when user or customer enter card into atm machine, the m pin get check by machine .if pin number and all user details are verify then the customer register phone number in bank that number will get otp of six digit and it is time base otp. the customer enter otp into atm machine and atm machine will run verification process of the otp and after sucessful verification of otp the user can withdraw cash from atm machine.

Keywords: - pin, dyanamic keypad , authentication, otp, security, verification, atm, verification, two factor authentication , overcome fraudulent use of atm .

LITERATURE SURVEY

The pin used in ATM is insecure because there may be chances of stealing ATM card and pin number. Many people normally choose easily guessed PIN's and passwords like birthday date, phone numbers and social security numbers, etc. OTP techniques can solve the issue of password.OTP is numeric string which randomly generated and sends to a registered number.To avoid misuse of ATM card additional we added additional feature otp and this otp is used in this project to overcome the problem.

Introduction

Nowadays, many people are dependent on computers for keeping major record of data. Data are sent in a costeffective manner across wider area network. Automated Teller Machine is the automatic systems being used since 1967 by many of us. ATM was found by John Shepphardbaren on June 1967 at United Kingdom. It emerged in India in 1968. Today, people have some secret number and password to protect their secret files and also for verification. The personal identification number is one of the day-to-day user authentication technique used in multiple situations, such as depositing and to drawback cash from automated teller machine (ATM), releasing lock in a mobile device, to proceed electronic atm transactions.

Security is provided to grant access to a legal user and to prevent the system from an illegal person. in public space Password authentication is often poses the problem of disclosure like key loggers installed on atm machine or a malicious onlooker who observes while the person enters the password. Virtual keyboards protection against key login but fail to avoid shoulder. In this system use to improvise these keyboards . When the user enters his PIN in the touch screen, immediately the numbers in the screen will be changed from its original position. The user entering next wouldn't have the same arrangement of numbers in the touch screen. Even when the Surfer observes the movement of the person entering the PIN number they can't able to hack the password. By using Node MCU 8266 IDE compiler with Node MCU 8266 it is efficiently possible to avoid Shoulder-Surfing attacks.

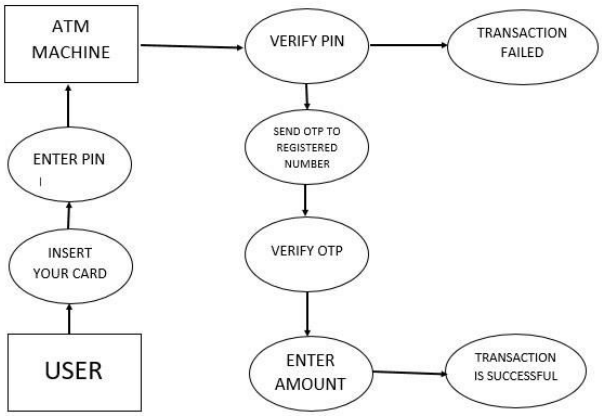
Methodology

We found that in almost every study it is mentioned that the security for ATM is provided by biometric systems but we have used a mechanism of two way authentication which provides more security and ensures safe transactions. It includes the use of PIN (Personal Identification Number) which is already provided by the bank and it is fixed for a specific user.

Once the PIN gets verified the OTP(One Time Password)is generated it is a randomly generated unique one-time-number/password which is used for providing second factor authentication service which reduces the vulnerabilities of biometric information.

Our system involves the concept of OTP(One Time Password) which is not present currently in the ATM systems .

2.2 BLOCK DIAGRAM



Block diagram 1.0

2.2.1 Textlocal API

With our Textlocal account you have user have to create API key , this enables user can integrate SMS services , software or CRM application in PHP any other .

Parameters

API key	special API key can create using this and forward to Control Panel for application. to do next process
Format	By default the format of response in json only.

Requests:- All requests sent using textlocal are consider . the command is the API that you call for execute, with included the POST parameters or GET parameters .

Responses:- by default, sent in JSON format. this can be changed to XML with the format parameter."status" field contain in Every response which can be either "success" or "failure". This field can be used to determine whether your request was successful.

Sender sms

Sender	it contain header and otp in it this field used by sender to specify the sender name which is approved by DLT and Textlocal. For otp messages, sender id of 6 numeric characters.
Message	Message content try to make simple as possible will less characters. It must be URL Encoded to support symbols like &.

Table 2.0

DLT REGISTRATION:

This registration is a block based registration . According to TRAI telemarketers have to be registered in the DLT The template will created in both DLT system and Textlocal site both the template will match exactly. The DLT will created heder as what u want that headar will paste in your message

It is issued to the public interest to control the SMS spam.

Earlier the bulk sms providers were required to register both the places in dlt and also in textlocal.

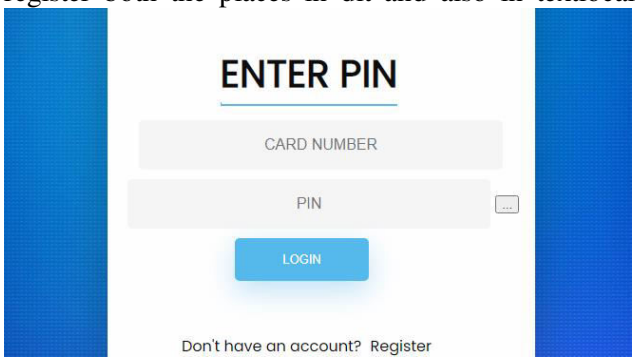


Fig : 1 Login Page

HARDWARE COMPONENTS:

Node MCU 8266:
ESP32 is a series of low-cost microcontrollers it contain integrated Wi-Fi and dual-mode Bluetooth. The ESP32 series a Tensilica Xtensa LX6 microprocessor in both dual-core and single-core variations and includes antenna , RF balun, power amplifier, low-noise receive amplifier, filters, and power modules. You tell your board what to do by sending a set of instructions to the microcontroller on the board.

RFID Reader : An RFID reader is the brain of the RFID system and is necessary for any system to function. it is also called interrogators devices that transmit and receive waves to communicate with RFID tags. RFID readers are divided into two types – Fixed RFID Readers and Mobile RFID Readers. readers that are fixed stay in one state and are mounted on stationary locations. An RFID reader is a reader with a antenna that includes one additional antenna port for the connection of an optional external antenna. Integrated readers are usually designed to be used for indoor applications without a high traffic of tagged items.

OTP
A one-time password is also known as one-time PIN or dynamic password, is a password that is valid for only one login session on a computer system .
OTP generation algorithms typically randomness, making prediction of successor OTPs by an attacker difficult, and also cryptographic hash functions. Which can be used to derive a value but are hard to reverse therefore difficult for an attacker to attack the data which should use.The advantage of otp is static password, therefore they cannot attack easily.
the hacker will try many time but it can't get the exact otp pin.

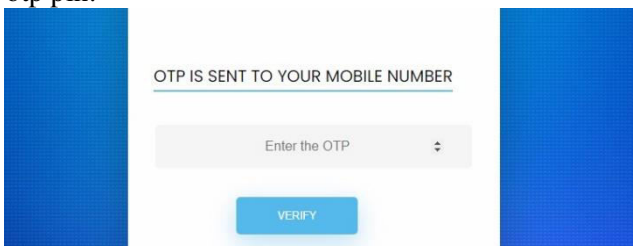


Fig : 2 Verification Page

Reading data from an RFID tag
After having the circuit ready, go to File > Examples > MFRC522 > Dump Info and upload the code. the reader and the tag closer to see all the information .

This is the information from the card u read , including the card UID that are in yellow. The information is stored in the memory and blocks as you can see in the previous data.
You have 1024 bytes of data storage and each sector is protected by two different keys that is A and B.

CONCLUSION

Therefore, the system ensures two times more security compared to the system we are currently using and does not require any kind of physical changes to the ATM machines we use nowadays.

Hence, this paper focuses on security of ATM system and even how to augment security for the ATM systems

REFERENCES

1) G.Nagarajan , S.Devi - "Improving ATM Security via Face Recognition", pp. 373 -376, IEEE 1995.

2) A.Taralekar , R. Tangade , G. Chouhan,-One Touch Multi-banking Transaction ATM System using Biometric and GSM Authentication, pp. 60 -64, IEEE , 2004

3) J. Soares , A.Gaikwad -Fingerprint and Iris Biometric Controlled Smart Banking Machine Embedded with GSM Technology for OTP, pp. 409 – 414, IEEE , 2006

4) R.Gusain , H. Jain , S. Pratap -Enhancing bank security system using Face Recognition, Iris Scanner and Palm Vein Technology, pp. 1 – 5 , IEEE , 1998

5) P. Adithya, S. Aishwarya, S. Megalai, S. Priyadharshini , Mrs. R. Kurinjimalar –Security Enhancement in Automated Teller Machine, pp. 21 - 25 , IEEE, 2002

6) Y. Xiao, Senior Member, IEEE-Differentiated Virtual Passwords, Secret Little Functions, and Codebooks for Protecting Users From Password Theft pp. 406 - 416 ,IEEE, 2012

7) V.Cherian Joseph, S.Dong-Myoung-Modeling "Agents for Public Environments to enhance the V20IP Embedded ATM Access Point Services ", pp. 672 - 675 , IEEE, 2010

8) G. Agrawal, A. Singh-Debit ATM card security based on chaos function and QR code pp. 372 - 376, IEEE , 2014