SECURITY AUTHENTICATION USING OTP

1. **R.CHANDRU.**

Assistant Professor of Electrical, Electronics and Communication Engineering, GITAM (Deemed To Be University), Rudraram, Patancheru mandal, Hyderabad, Telangana, 502329, INDIA.

2. **KALVAKUNTA MEGHANA** ,
3. **PULLURI RAJESH,**
4. **RANGA SRINIVAS LOHITH,**
5. **VEDANTHAM NAVADEEP**

Department of Electrical, Electronics and Communication Engineering, GITAM (Deemed To Be University), Rudraram, Patancheru mandal, Hyderabad, Telangana, 502329, INDIA.

Abstract

There are many authentication schemes that are in practice today. If they are categorized based on usability and security then most of them fall into the category of security that ensures the safety of the user's account using second factor, but they lack proper usability. The remaining are the authentication schemes that are designed to achieve better usability, but lack proper security to protect the user from communication channel attacks and masqueraded server attacks. This research was aimed at providing authentication schemes that shall bridge the gap between security and usability. The idea of the project is to setup a Security system which is more secured for a door lock or a bank locker. The idea is to design a prototype using a onetime password (OTP) to unlock. This is an embedded system which helps to increase the security.

Keywords:
Node Micro-controller (ESP 32S CHIPSET) , LM 2596 . LCD (16 X 2), I2C MODULE, SERVO MOTOR (SG-90), 4 X 4 MATRIX KEYBOARD, POWER SUPPLY.

1. Introduction:

Access controls exist to prevent unauthorized access. Companies should ensure that unauthorized access is not allowed and also authorized users cannot make unnecessary modifications. The controls exist in a variety of forms, from Identification Badges and passwords to access authentication protocols and security measures.

BACKGROUND WORK:

There are few systems using this principle. In this project, there are things that were made sure that this becomes handy and more secure. Hence, we've decided to make an application and use the secured database which is free and easy to use.

Features of this unit are:
1. Safe & Secure
2. Easy & affordable.

PROPOSED SYSTEM

Using the Node MCU, we program it to unlock only when the specific OTP is entered, which is generated in the database in the "FIREBASE". The OTP will be displayed from an android application and when the OTP is entered, the door gets unlocked.

2. Literature Survey

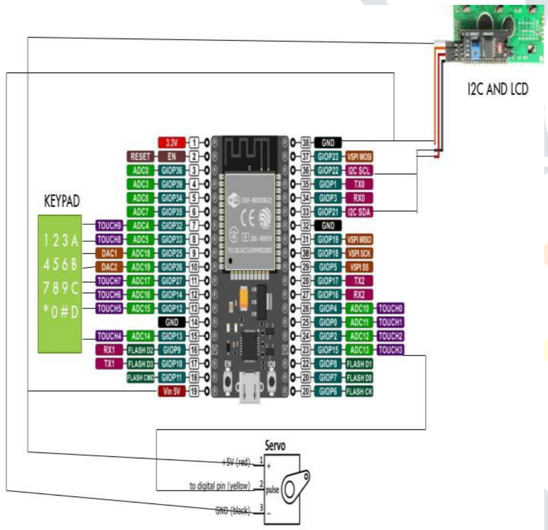
A user authentication is a process to prove that whether a certain user is authorized to use a target service or system. There are various user authentication methods such as knowledge-based authentication, ownershipbased authentication and attribute-based authentication. Among them, knowledge-based authentication is widely used these days, such as ID/PASSWORD in most websites or services. However, the password is maybe predictable because it should be easy for users to memorize. Thus, an adversary could get the passwords of users by brute-force attack in a short period of time. A Two-Factor Authentication (TFA) can be used as a countermeasure to this weakness. Especially, OTP (One Time Password) protocol is the most widely used for TFA with user's ID/PASSWORD .

In 2012, Hoyul Choi, Hyunsoo Kwon, Junbeom Hur, have presented a paper "A Secure OTP Algorithm using Smartphone application". In this paper, authors have proposed, An OTP Algorithm which uses Captcha Image, IMSI number, Limited Time availability to make it secure against Man in the Middle and Man in the Phone Attacks, using Smartphone Application.

In 2014, Dr. Ananthi Sheshashayee, D. Sumathy, have presented a paper "OTP Encryption Techniques in Mobiles for Authentication and Transaction Security"

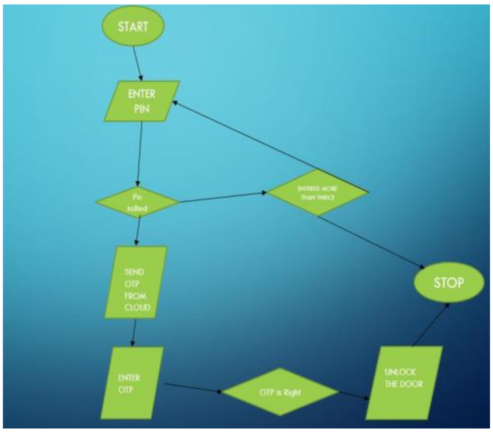
In this paper, authors have proposed Two Factor Authentication using PIN (Personal identification Number) and OTP (One Time Password. In 2013, Ms. Kalaikavitha, Mrs. Juliana Gnanaselvi, have presented a paper "Secure Login Using Encrypted One Time Password (OTP) and Mobile Based Login Methodology". In this paper, the approach of using AES (Advanced Encryption Standard) Algorithm for Encrypting OTP has been proposed.
In 2010, Li Yinxiang, Lizhi Zhong presented paper titled "Research on S/Key One Time Password Authentication System" in which they propose the use of HASH function for generating OTP .

3. Implementation:



The controlling device of the whole project is Node Micro-controller (ESP 32S CHIPSET) . Servomotor, 16*2 LCD display is interfaced to the MICROCONTROLLER. When the user enter the pin number through keypad then the user get the OPT and again user enter the OTP the bank locker is unlocked if the OTP is correct.

FLOWCHART OF WORKING



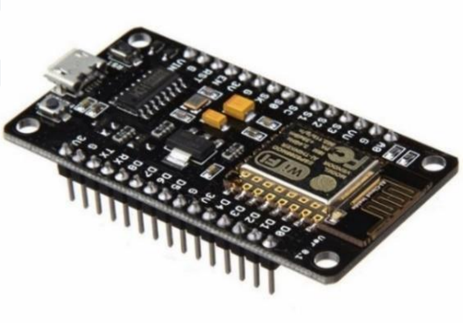
4. Related Work:

The brief introduction of different modules used in this project is discussed below:

POWER SUPPLY:

The power supply was given to the board via 5V DC adapter according to the required specifications.

Node MCU:



The internal flash of the ESP32 module is organized in a single flash area with pages of 4096 bytes each. The flash starts at address 0x00000, but many areas are reserved for Esp32 IDF SDK and Zerynth VM. There exist two different layouts based on the presence of BLE support. The ESP32 chip integrates a dual-core processor with 448 KByte ROM, 520 KByte SRAM, 16 KByte SRAM in RTC, 802.11 b/g/n/e/I Wi-Fi, Bluetooth v4.2

BR/EDR & BLE, clocks & Times, abundant peripheral Interfaces and sercurity mechanism.

Features:

NodeMCU based on ESP-WROOM-32 module

Based on ESP32 DEVKIT DOIT

- 30 GPIO Version
- ESP32 is a dual core 32-bit processor with built-in 2.4 GHz Wi-Fi and Bluetooth
- 4MByte flash memory
- 520KByte RAM
- 2.2 tp 3.6V Operating voltage range
- In breadboard friendly breakout
- USB microB for

LM 2596:

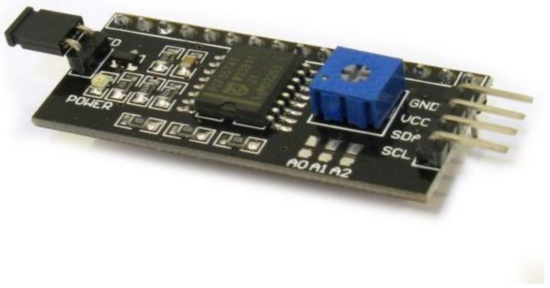
This is an LM2596 DC-DC buck converter step-down power module with high-precision potentiometer for adjusting output voltage, capable of driving a load up to 3A with high efficiency. When the output current required is greater than 2.5A(10W) an external heatsink is suggested. Use on board switch to change display measurement between the input or output voltage, and a LED indicate which value(IN/OUT) is being measured. This setting is stored even after power off. Voltmeter can be turned off, just keep the switch pressed for 1 second and leave it. Adjust Input and output voltage measurement error offset – long press switch for 4 seconds or more, the digital display flashes, then short press the button to change the value of output (values range from -0.5 to 0.5, the unit is V), a positive number indicates an upward calibration, negative downward

LCD (LIQUID CRYSTAL DISPLAY) :

One of the most common devices attached to a micro controller is an 16x2 LCD display.This means 16 characters per line by 2 lines. There are totally 16 pins in an LCD Display. You can use directly all the pins in 8-bit mode with Arduino or 12 pins using 4-bit mode. In this tutorial, we use the I2C module for LCD and multiplex it into just 4 pins. This pin details might not be useful while using I2C Method but this is the actual pin details of all the pins in LCD Display. The project status will display on LCD.

I2C MODULE:

This 3-byte sequence sets all bits of a PCF8574 I/O expander chip low. All 3 bytes should be sent to the USB-I2C in one sequence. A gap will result in the USB-I2C re-starting its internal command synchronization loop and ignoring the message. After all bytes have been received the USB-I2C performs the IC2 write operation out to the PCF8574 and sends a single byte back to the PC. This returned byte will be 0x00 (zero) if the write command failed and non-zero if the write succeeded. The PC should wait for this byte to be returned (timing out after 500mS) before proceeding with the next transaction.



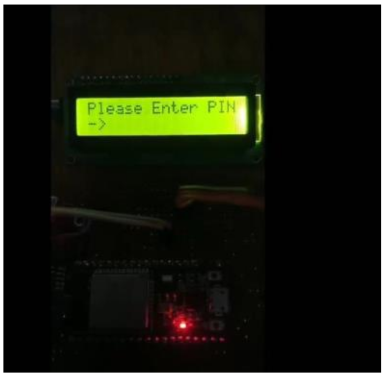
SERVO MOTOR (SG-90)

Micro **Servo Motor SG90** is a tiny and lightweight server **motor** with high output power. **Servo** can rotate approximately 180 degrees (90 in each direction), and works just like the standard kinds but smaller. PWM signal produced should have a frequency of 50Hz that is the PWM period should be 20ms. Out of which the On-Time can vary from 1ms to 2ms. So, when the on-time is 1ms the motor will be in 0° and when 1.5ms the motor will be 90°, similarly when it is 2ms it will be 180°. So, by varying the on-time from 1ms to 2ms the motor can be controlled from 0° to 180°

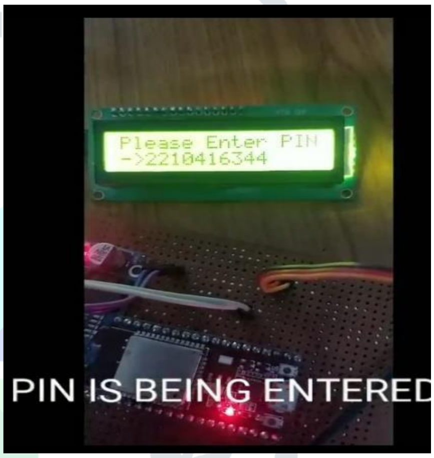
4X4 MATRIX KEYBOARD:

Keypads are mostly used as user input. The 4x4 matrix keypad uses the 16 keys, but yet the 8 output pins are used in the interface to the micro controller.A Matrix keypad is the most commonly used input device in many of the application areas like digital circuits, telephone communications, calculators, ATMs, and so on. A matrix keypad consists of a set of push button or switches which are arranged in a matrix format of rows and columns. These keypads are available in configurations like 3×4 and 4×4 based on the application it is implemented for

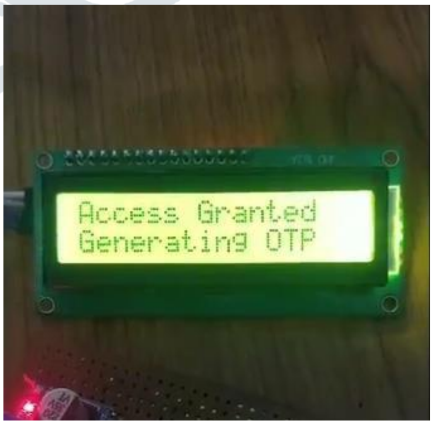
4. RESULTS:



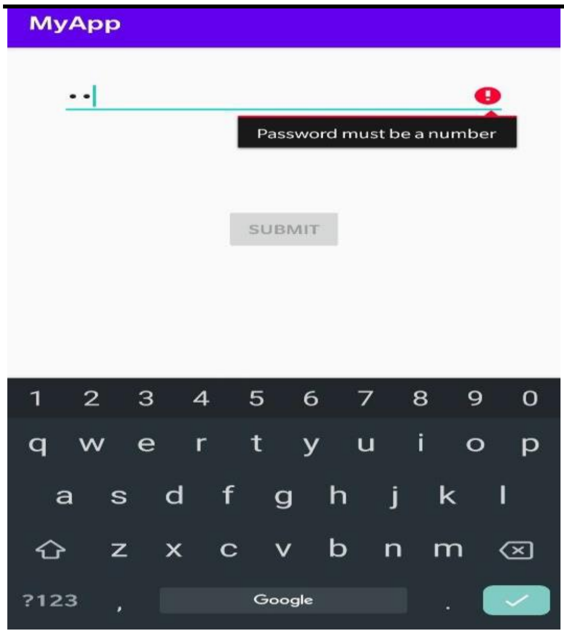
It displays to enter the PIN



PIN is entered

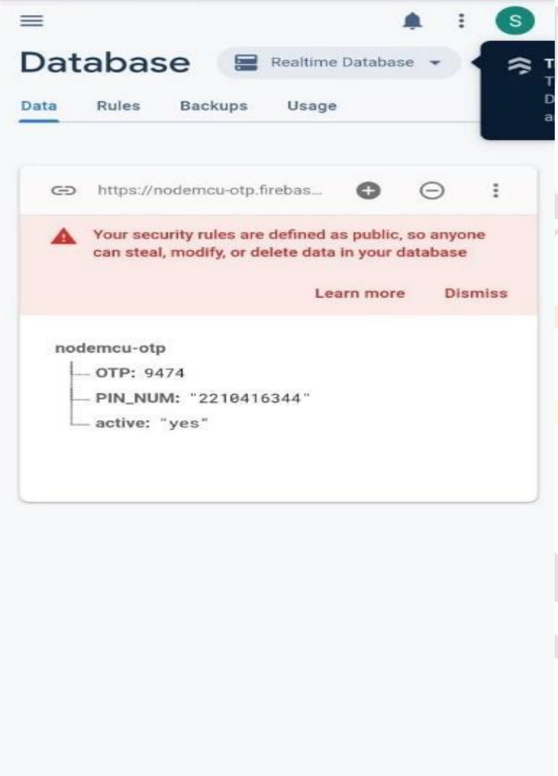


Access is granted if PIN is right


MyApp

Password must be a number

PIN must be a Number


Database

https://nodemcu-otp.firebas...

Your security rules are defined as public, so anyone can steal, modify, or delete data in your database

```
nodemcu-otp
├─ OTP: 9474
├─ PIN_NUM: "2210416344"
└─ active: "yes"
```

Redircted to OTP page

```
Enter your OTP
->5339
```

Entering OTP

```
Unlocking Doors
```

The doors get unlocked

The motor rotates which opens the doors

5. CONCLUSION:

The existing model presents an Integrating feature of all the hardware components which has been used and developed in it with Node Micro-controller (ESP 32S CHIPSET). The Presence of each and every module has been reasoned out and placed very carefully. Hence the contributing to the best working unit for “SECURITY AUTHENTICATION USING OTP” has been designed perfectly. Thus, the project has been successfully designed and tested.

5. ACKNOWLEDGEMENT

We would like to thank all the authors of different research papers referred during writing this paper. It was very knowledge gaining and helpful for the further research to be done in future.

REFERENCES

[1] The Fourth International Workshop on Computer Networks & Communications Research paper.

[2] Nir Kshetri and Jeffrey “Voas Blockchain-Enabled E-Voting” ,*IEEESOFTWARE.*

[3] Haikel Magrahi, Nouha Omrane, Olivier Senot, Rakia Jaziri, "NFB: A Protocol for Notarizing Files over the Blockchain", *2018 IEEE*

[4] Yi-Hui Chen, Shih-Hsin Chen, Iuon-Chang Lin, "Blockchain based Smart Contract for Bidding System", *Proceedings of IEEE International Conference on Applied System Innovation 2018 IEEE ICASI 2018- Meen, Prior & Lam (Eds)*