ISSN No:-2456-2165

Desktop and Mobile Application based Three Step Security System

Tiasha Banik, Trisha Das, Srabani Biswas, Sayan Majhi, Tushar Kundu Aniruddha Ghosh, Mainuck Das, Arindam Banerjee
Dept. of ECE, JIS College of Engineering, Kalyani

Abstract:- The main objective of this paper is to propose a new design for a door locking system that involves a three-step process using desktop and mobile application. To achieve this, two separate applications have been developed, one for the desktop and another for the mobile device. The desktop application has been specifically designed for the Raspberry Pi device, while the mobile application uses Bluetooth technology for its implementation. The system utilizes an Arduino microcontroller as the hardware component, although the desktop application can also be implemented on a Raspberry Pi microprocessor.

In this proposed system, the user is required to complete the first two steps of the process, which involve setting up a user ID, password, and a security question. The final step involves authentication through the use of a one-time password (OTP). This three-step process is designed to enhance security and provide greater protection against unauthorized access to the locked door.

It is important to note that this proposed design is unique and has not been reported previously in any other research work. The use of a desktop and mobile application, combined with the implementation of a three-step process using an OTP, provides an innovative and effective approach to door locking systems.

Overview of Technology: The Desktop and Mobile Application Based Three Step Security System is an innovative project that utilizes various technologies to provide enhanced security for users. Here is an overview of the technologies used in this project:

- **Desktop Application: The desktop application in this system is designed for the Raspberry Pi device. The application is developed using Python programming language and utilizes the PyQt5 library for graphical user interface (GUI) development. The desktop application provides a user-friendly interface for users to set up their security credentials and manage their account.**
- **Mobile Application: The mobile application is implemented using Bluetooth technology, which allows for secure communication between the mobile device and the Arduino microcontroller used in the system. The mobile application is developed using Android Studio and Java programming language. The mobile application enables users to receive OTP and authenticate themselves.**
- **Arduino Microcontroller: The Arduino microcontroller is the hardware component of this system. The microcontroller is programmed using C++ programming language and is responsible for managing the authentication process.**

Keywords:- *Desktop Application, Mobile Application, Python, Arduino, Raspberry Pi, Bluetooth.*

I. INTRODUCTION

The advantage of technology has brought about numerous challenges to security systems due to the prevalence of cybercrime. In response, various security systems have been designed to provide protection to the general public . One such system that has proven to be effective is the OTP-based system, which is widely used in ATM machines and other devices. Previous research works have presented wireless security system designs, such as the use of Bluetooth technology for a Wi-Fi security system, the use of an ESP-32 based Spy-Cam and a GSM module (which can be costly), and the use of Bluetooth technology. However, this paper proposes a novel approach using desktop and mobile applications that are based on an OTP system. The proposed system is a new and innovative solution to security systems, and to the best of the authors' knowledge, has not been presented before.

II. CREATION OF DESKTOP APPLICATION

A desktop application has been developed using the python programming and the wx python library, which can be utilized on both desktop and Raspberry pi devices for hardware implementation. The application takes input from the user in the form of a login id, password, security question, and OTP (One Time Password). If the input is correct, then the user is logged in and an OTP is generated, which the user needs to enter to unlock the device.

- **Algorithm 1:**

The Algorithm 1 of the application is as follows:

Input: login id, password, security question (pet name), OTP.

Output: OTP generated, unlocked.

Variable: x, y, z

X= prefixed id;

Y= prefixed password;

Z=prefixed security question (pet name);

if ((login id==x) && (password==y) && (security question==z))

{

OTP generated = generate OTP ();

```
if (OTP==OTP generated)
Unlocked= true;
}
else
{
Unlocked= false;
}
Generate OTP ()
{
variable a= [OTP strings are stored here];
integer i= random (size of a);
return a[i];
}
```

The application window has three text boxes for collecting user id, password, and security question (pet name). Once the user gives the correct input and presses the "SUBMIT" button, the information is checked. If it is found to be true, a dialogue box is displayed showing the "Successful Log in", and an OTP is displayed in the label below the "SUBMIT" button. Otherwise, the dialogue box shows the "Unsuccessful Log in". The OTP is entered by the user in the text box provided and upon pressing the "UNLOCK" button, another dialogue box is displayed showing the unlocking information.

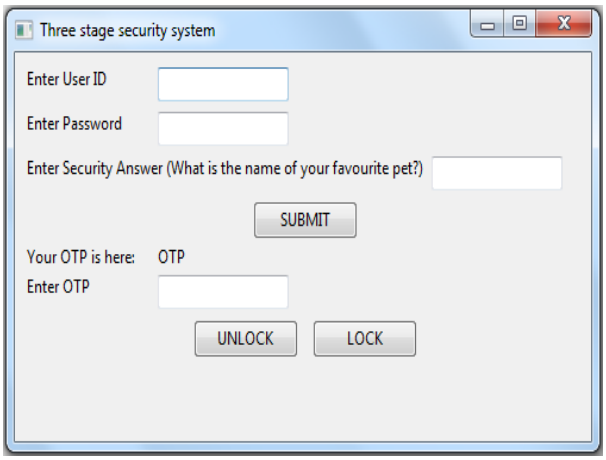

Fig. 1: Application Window

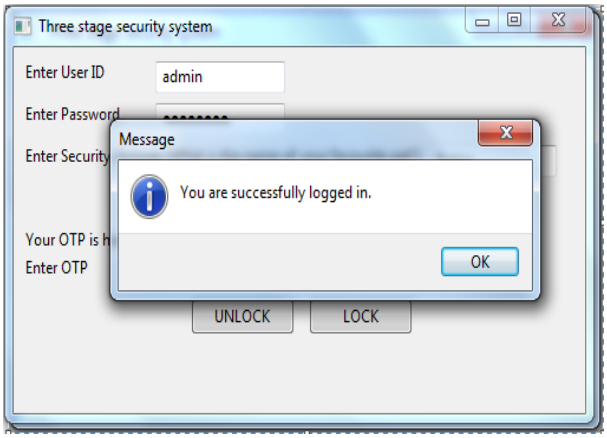

Fig. 2: Dialog Box in the main application

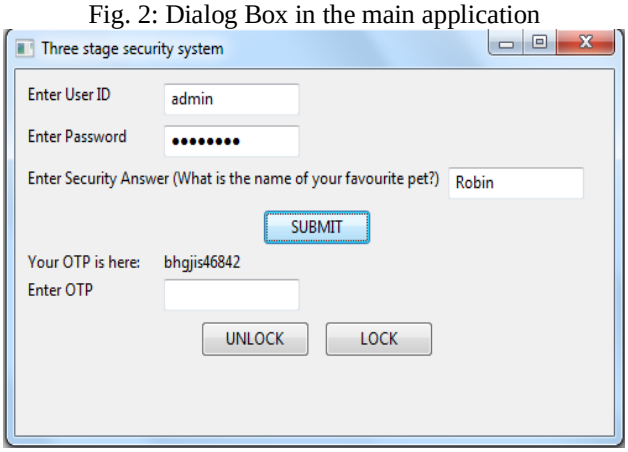

Fig. 3: OTP display in the label

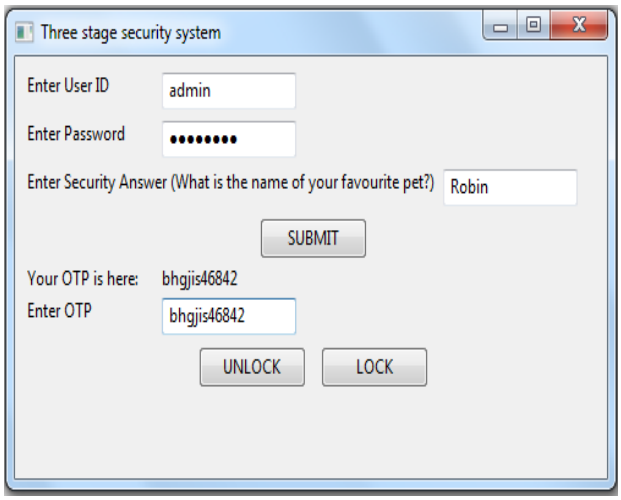

Fig. 4: OTP is entered in the text box

ISSN No:-2456-2165

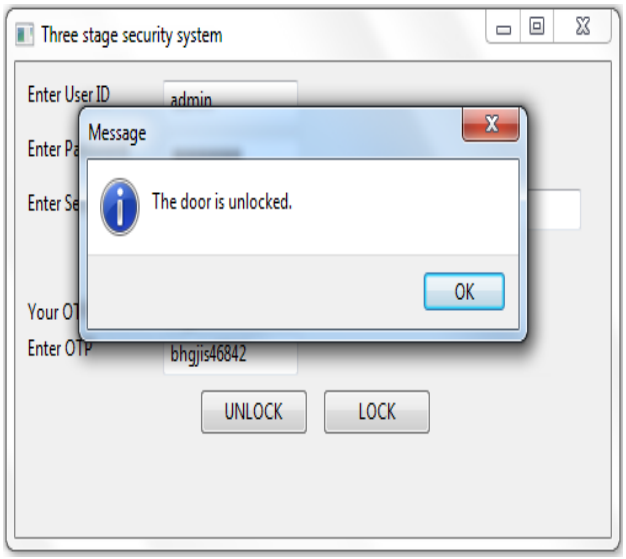

Fig. 5: Dialog box shows the unlocking information after the UNLOCK" button is pressed after entering the OTP

When the "UNLOCK" or "LOCK" button is pressed, a string data is transmitted to the microcontroller for necessary hardware operation. The string data is converted to byte from using UTF-8(Unicode Transformation Format) and then transmitted to the microcontroller. The necessary library for converting the string data to UTF-8 format is "pyserial".

The hardware components of the system include an Arduino microcontroller (either the Uno or Mega), a servo motor, a liquid crystal display (LCD), and an I2C module called PCF8574. The I2C module enables communication between the Arduino microcontroller and the LCD display using the I2C protocol. The Arduino microcontroller has two dedicated pins for I2C communication, which are called SDA (Serial Data Adaptor) and SCL (Serial Clock). These pins are used to connect the LCD module to the I2C module and establish communication between the two. Figures 6 and 7 demonstrate the hardware interface and simulation results for both an open and closed door.

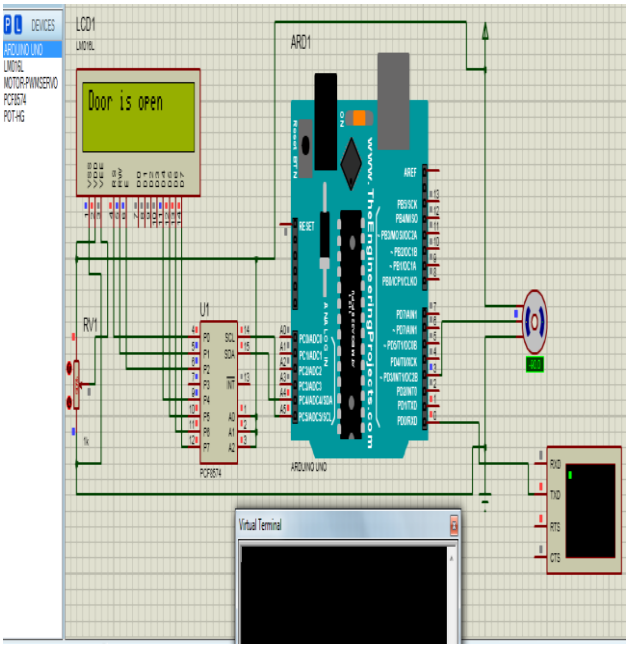

Fig. 6: Hardware implementation showing open door

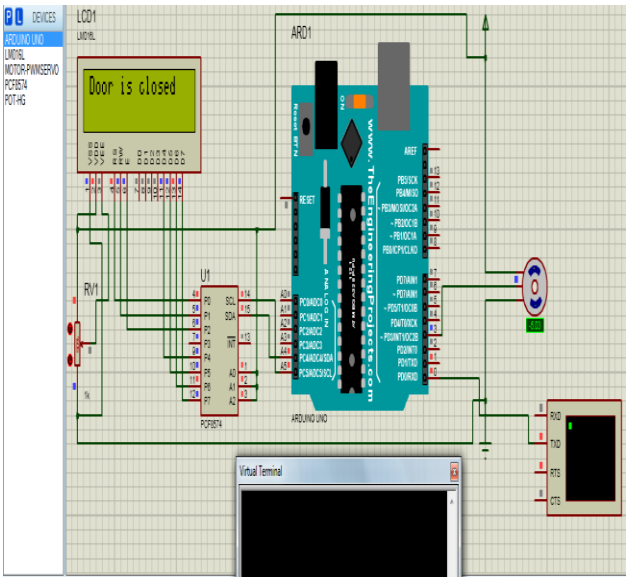

Fig. 7: Hardware implementation showing closed door

A locking/unlocking system has been created using a servo motor, which is an actuator controlled by a Pulse Width Modulation (PWM) signal. The motors rotation is dependent on the pulse width of the signal, and it has been incorporated into the design of the system.

To begin the process, byte-form serial data is transmitted to the microcontroller and is then converted into a string or integer format through the activation of serial communication. It is important to ensure that the COM port and BAUD rate specified in the pyserial library initialization match those used in the communication.

The following algorithm (Algorithm-2) outlines the detailed process involved in the creation of the locking/unlocking system.

- **Algorithm 2:**

Input: int st;

```
Output: servo, lcd
While(true)
{
if (Serial.available())
{
        St=Serial.parseInt();
}
if(st==1)
{
        Servo movement to unlock;
        Lcd display (UNLOCK);
}
else if(st==2)
{
        Servo movement to lock;
        Lcd display (LOCK);
}
}
```

III. MOBILE APP CREATION

Based on the algorithm presented in Algorithm 1, a mobile application has been created using the MIT App inventor tool, which is an online platform for designing mobile applications.

The application window, as shown in the fig 7, works with the help of a Bluetooth device.

The first component in the application is a list picker that allows the user to select the appropriate Bluetooth device for the application. The MIT App Inventor platform provides a "BluetoothClient1" component that facilities Bluetooth communication. Additionally, there are three text boxes in the application: the first for providing the user ID, the second for the password (displayed as dots for security),and the third for the security question, known only to the user.

When the user enters all the required information and presses the "Submit" button, the application verifies the information against the predetermined data. If the data is verified, the microcontroller generates a random OTP using algorithm-3 and transmits it to the application,where it is displayed in a label.

- **Algorithm 3:**

```
Input: int st;
Output: servo, seven segment (bit vector);
Variable: otp [choose array size] ={Strings to send};
while(true)
{
        if (Serial. available ())
        {
                st=Serial.parseInt();
        }
        if(st==1)
        {
                Serial.print(otp [random (array size)]);
        }
        else if(st==2)
        {
                Servo movement to unlock;
                seven_segment display(1111110);
        }
        else if(st==3)
        {
                Servo movement to lock;
                seven segment display (1001110);
        }
}
```

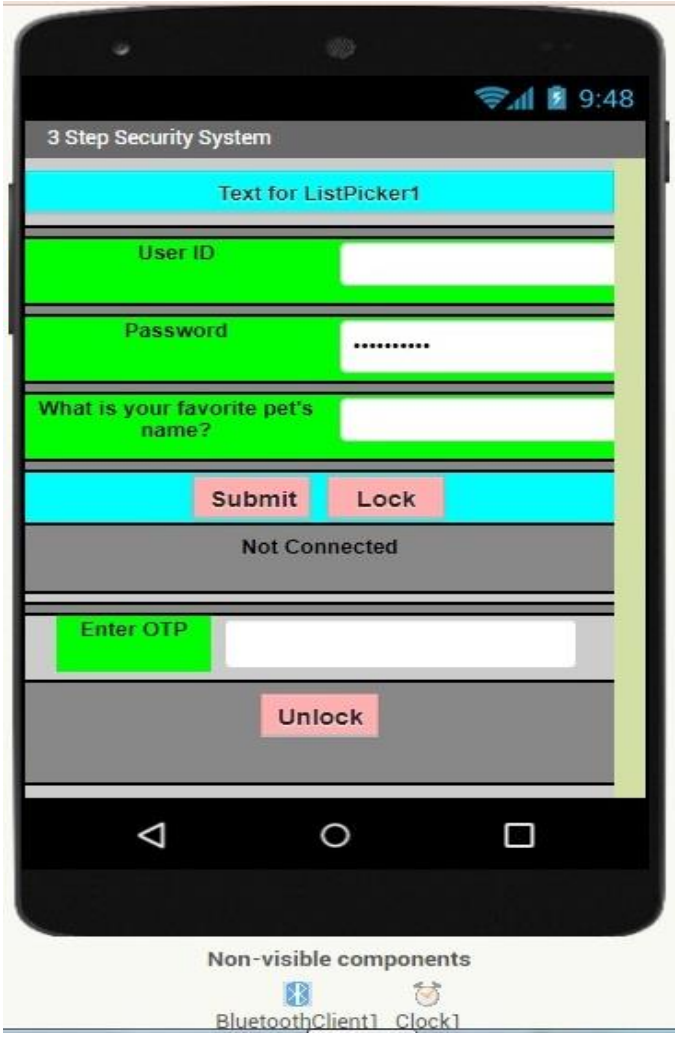

Fig. 8: Mobile Application Window

IV. CONCLUSION

The paper presents a three-step security system based on One-Time Password (OTP) technology, which utilizes both desktop and mobile applications. The authors developed individual applications for each platform and demonstrated separate hardware setups for the two types of applications. Additionally, it was noted that the desktop application can also be implemented on a Raspberry Pi device. The work was exclusively new to the best of the knowledge of the authors.

ACKNOWLEDGMENTS

The authors are grateful to the authority of JIS College of Engineering to encourage them to perform the research and development.

REFERENCES

[1.] Sinha, A. K.: https://www.electronicsforu.com/electronics-projects/otp-based-smart-wireless-locking-system
[2.] Falohan A. S., Makinde B. O., Adegbola O. A., Akin-Olayemi T. H., Adeyege A. E., Adeosun A. E. and Akande B. E.: Design and Construction of a Smart Door Lock With an Embedded SPY-Camera. In: Journal of Multidisplinary Engineering Science and Technology, Vol. 8, no. 7. July (2021) 14521–14528
[3.] Rajiwade B., Thakar S., Pokharkar P. and Malbhare S.: Design and Implementation of Smart Door Lock Control Systemusing Bluetooth Controller of Smart Phone. International Research Journal of Engineering and Technology, Vol. 3, no. 11. November (2016)