iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 Issue: VII Month of publication: July 2023

DOI: https://doi.org/10.22214/ijraset.2023.54794

Two Step Authentication System based on OTP & Gesture Recognition Based on Accelerometer

Ahwas Altaf Zargar[1], Syed Kashif Jeelani Alvi [2]
[1]*B. Tech Electronics and communications, University of Kashmir*
[2]*M. Tech Microelectronics, NIT Srinagar*

Abstract: The paper discusses the use of two step authentication system in- stead of traditional single step such as biometric, password etc. The paper discusses the disadvantages of using existing single layer security in everyday security needs. Further the paper proposes the idea how a Two-step authentication system based on pattern recognition and OTP (One Time Password) would create a more robust and secure authentication system while being cost effective and re- quiring less electronic components. The first layer of security is achieved by pattern recognition by pattern recognition we mean a user draws a pattern in air and using Arduino & ADXL35 (3-axis accelerometer) module we can deduce the pattern .The accelerometer is used to track the X,Y values obtained from the module and using these values we ascertain whether the pattern created by the user is accurate. As for the second layer we use Arduino as a random number generator & SIM7100A (4G SIM module) serves the purposes to send data to the user via SMS.

Keywords: Arduino, OTP, Hand Gesture, Security

I. INTRODUCTION

As security is the foundation that keeps many sectors afloat, from locks for doors and gates to significant financial institutions like banking, it is crucial that we strengthen our security with better technology and processes to create a robust and efficient systems. The paper's major goal is to create a security system that is more effective and reliable. The paper will demonstrate how a successful security system may be created using small, affordable components.

II. PROBLEM STATEMENT

In these times security is a big concern. It has been noted that all currently proposed security solutions are either readily circumvented or extremely expensive, making them unsuitable for daily security demands like an ordinary door lock on a residential building. We assess the current authentication strategies and go over the associated problems.

A. Biometrics

Biometrics is a term that refers to measuring unique individual characteristics such as the retina, the iris, fingerprints or even the face. Today, the term is generally used by most people to describe a method for securing computers and stored data requiring a user to undergo a scan of the body part used for recognition. While many security system use biometrics but better security system add an additional layer of security by biometrics + password authentication. This method has the drawback that it necessitates specialized scanning equipment, which is not suitable for many industries and can be prohibitively expensive for small enterprises.

B. Token Authentication

Tokens are physical objects that are used to enter secure systems. Dongle, card, and RFID are examples of common forms. Since a hacker needs long credentials and the tangible device itself, which is far more difficult for a hacker to obtain, a token makes it more challenging for a hacker to access an account. Disadvantages: Unfortunately, the user can quickly weaken this authentication approach. A token is simply something you can lose. Even the most careful people can forget something in a car that is then stolen, lose something in their pocket while out to dinner, or leave something on a key ring or in a briefcase.

C. Password Based Authentication

The most used form of authentication is passwords.

A string of letters, numbers or special characters can be used as a password. Even though better passwords are formed these days by using capital letters in addition with special strings such as @, # etc. But still passwords have drawbacks such as poor password habits such as keeping 1234 as a password, too many security systems use password authentication due to which several passwords need to be remembered which becomes inconvenient for the user.

III. METHODOLOGY

A. Hand Gesture Recognition (Pattern Recognition)

This method is basically drawing pattern in the air tracking the X,Y,Z values of the user's hand obtained using ADXL35 comparing these values with the already stored pattern in the system for verification. Any pattern can be mapped to the X,Y values obtained from the sensor. The system records the changes made in these values during the formulation of the pattern and it compares the changes that occur when the user makes a pattern ,if the changes occur in same order as the previously stored pattern, then it can be safely said that the user has drawn the same pattern as stored in the system. Further it is worthy to mention that Z values from the sensor are ignored as it only increases the complexity of the system .It can be thought of as the system marks the (X,Y) coordinates of the hand which it later uses to interpret whether the pattern draw is correct or not.

B. OTP authentication

To generate a random number using Arduino a built-in function called random(),randomSeed() can be used but these generates a pseudo random number which means it generates a series of random numbers which are pre-determined and not actually random but closely approximated to series of random numbers. We propose using analogRead() function of Arduino to generate a random number. The analogRead() will be used to read values between 0 to 1023.The Logic used to map analog values to digital output will be used meaning float voltage= sensorValue * (9.0 / 1023.0); int value = round(float voltage); Convert float values to integer.

The above equation will map each sensorvalue to a range of 0-9

The Values obtained from the above algorithm will be used and sent to mobile phone using Arduino + SIM7100A (4G module) to send the OTP using SMS. After receiving the OTP, the user needs to enter the OTP obtained in the keypad attached to the Arduino for verification. After verification the lock will open

C. System Implementation

The system was implemented using the following hardware.

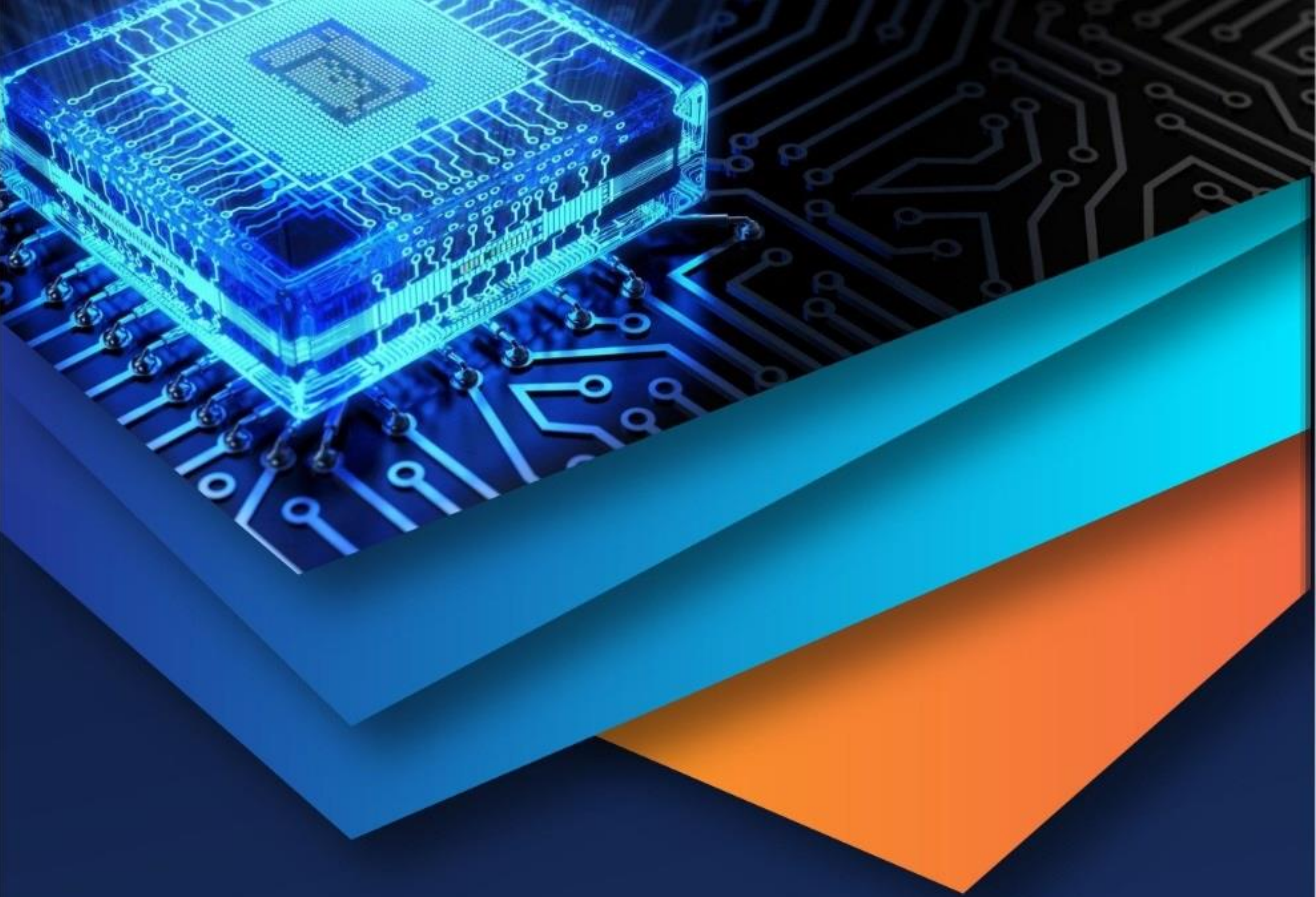
1) *Arduino UNO:* Arduino UNO is a microcontroller which serves as the brain of the project.
2) *SIM7100A:* It is a 4G SIM Module. It acts as a gateway between Arduino & the internet. It's used to connect Arduino UNO to the internet.
3) *Keypad:* A 12 button keypad has three columns and four rows. The purpose of keypad is to input the passcode.
4) *OLED:* OLED is used as a screen in the project which displays information on it.
5) *ADXL35:* The ADXL335 is 3- axis. The accelerometer is used to track hand movements in this project.

IV. CONCLUSIONS

Security is only necessary for precious objects, such as gold and diamonds, which range in size from small but priceless to bigger and more significant costly items like houses, cars, etc. Therefore, having a system that is more reliable and secure is always desirable. The proposed approach includes two-step verification, increasing security measures by offering two layers of security in place of the more common one. Additionally, the system's usage of small, affordable electronics components expands the system's use in several security-related fields.

REFERENCES

[1] https://www.idrnd.ai/5-authentication-methods-that-can-prevent- the-next-breach/
[2] https://www.alliancetechpartners.com/network-security-authentica- tion/



10.22214/IJRASET

INDEX COPERNICUS
45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL
IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY