iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50421

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

Design and Implementation of an IOT Enabled Classified Authentication System using LabVIEW

Dr. Amit Gangopadhyay
Professor, Department of Electronics and Communication Engineering, School of Engineering, Mohan Babu University, Tirupati, Andhra Pradesh, India

Abstract: ***This paper describes the development of an authentication system with Internet of Things (IOT) enabled solution and the dashboard support with mobile applications. This Authentication system is composed of NI myRIO embedded controller with the proximity detection sensor, which senses the presence of the person in front of the device setup. After sensing a person in front of the system, GSM module is utilized to send the unique One Time Password (OTP) to the owner of the system for accessing and will provide an option of entering the OTP through the assembled thumbwheel switches. Once after entering the password, on board button of NI myRIO has to be pressed to make an entry of the password into system. If password matches with master database OTP, authentication will be provided to the end user along with LED glowing status and motor rotation will be turned on. If the password doesn't match with the master database password, the buzzer will be blowing indicating the authentication failure that means access denied. In both the cases the data will be updated to cloud through dweet IOT service and the same status can be even updated into dash board application.***
Keywords: Authentication System, Internet of things, Sensor, Labview, Embedded Controller

I. INTRODUCTION

Today, in this digital world, privacy and security have become one of the essential elements for an individual or an organization [1]. Security systems have emerged from completely mechanical security systems, mechanical subsystems, partially digital and completely digital with IOT being enabled to the authentication system and enabling real time monitoring and remote access of an individual system or an organization [2-3]. Security risks have also increased with the advancements in the technology and easier and open source knowledge available to elude the authentication mechanisms and security systems.

Authentication system is more useful and important now than ever before, due to the increase in the number of single household livings [4]. The fear of unknown and anxiety is making it hard for people who are living alone. Also, in this present generation there is a gradual increase in thefts where it caused fear to the people. The crime rate has also increased in an alarming state, so it is safer to have a highly secured home, office, anything that needs to be protected [5].

Security systems can be a crucial design element in various applications. This paper described the authentication process completely depends on the generation of a onetime password, which is unique and shall be notified to the owner via a text message for granting the access. The complete authentication details will also be logged to the cloud, which would provide all the insights in case of any authorized or unauthorized access of the system [6].

This is very unique and is definitely not vulnerable to cyber attacks. The Internet of Things is also a very promising technology that can be relied upon [7-8]. The system can resist the common attacks and successfully provide real time image proctoring as well. The use of dashboard helps it easy to read all the information that is stored. This authentication system can also be applied to various sharing economy platforms such as lodging facilities and personal lockers. This system allows single-person residents to relieve the anxiety caused by the password leakage and unforeseen visitors, making solve the growing social problems occurring in single person households.

II. SYSTEM DESIGN

Classified authentication system involves the design of hardware and software. The hardware components which has been used are camera , LEDs, motor driver ,buzzer, IR sensor, GSM module and the most crucial component NI myRIO which is an embedded device made by National Instrument (NI). It was applied to integrate the components and to transmit the specified data to the web application through wireless platform. It integrate the sensors and wireless platform in order to provide acquire specified data. Data can be visualized, organized, secured, analyzed and collected in real time. Dashboard is a tool used to make the information collected from connected smart devices into a human-readable language.

©IJRASET: All Rights are Reserved

The performances are recorded through Internet of things (IoT) where the meaningful data and location can be viewed through IoT platform. The chosen IoT platform is Ubidots. IoT dashboard is a control panel for IoT devices or a tool in the form of a web app which is associated with the smart devices and IoT systems. This proposed system was designed and constructed using LabVIEW graphical Programming Language which is feasible and user-friendly. LabVIEW is an integrated development environment designed specifically for engineers and scientists. Native to LabVIEW is a graphical programming language that uses a dataflow model instead of sequential lines of text code, empowering to write functional code using a visual layout that resembles our thought process. Dweet platform are used for the storage of information about the transactions of successful and unsuccessful authentication attempts. The overall system is shown in Fig.1 and the schematic diagram as shown in Fig 2.

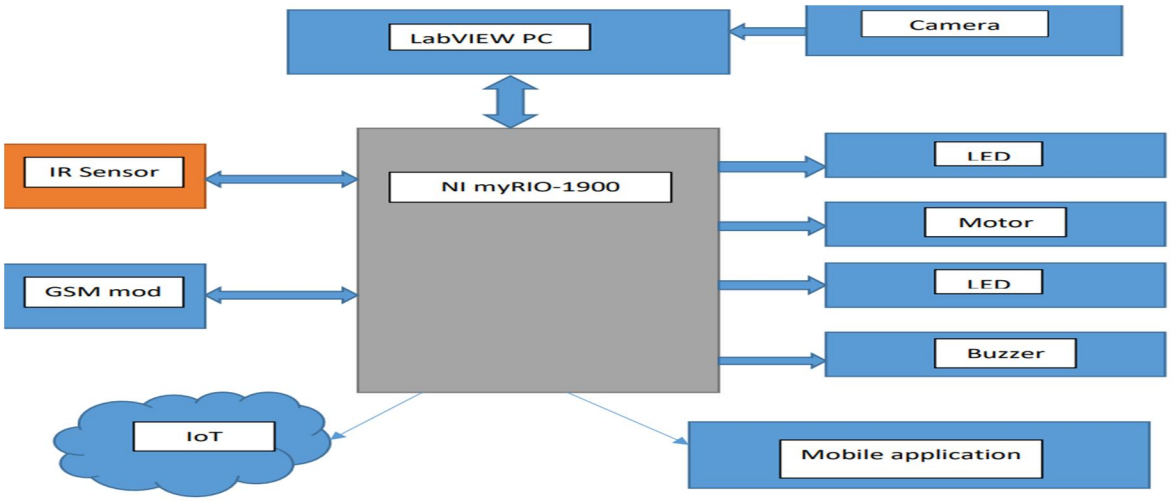


Fig.1 Block Diagram of the overall system

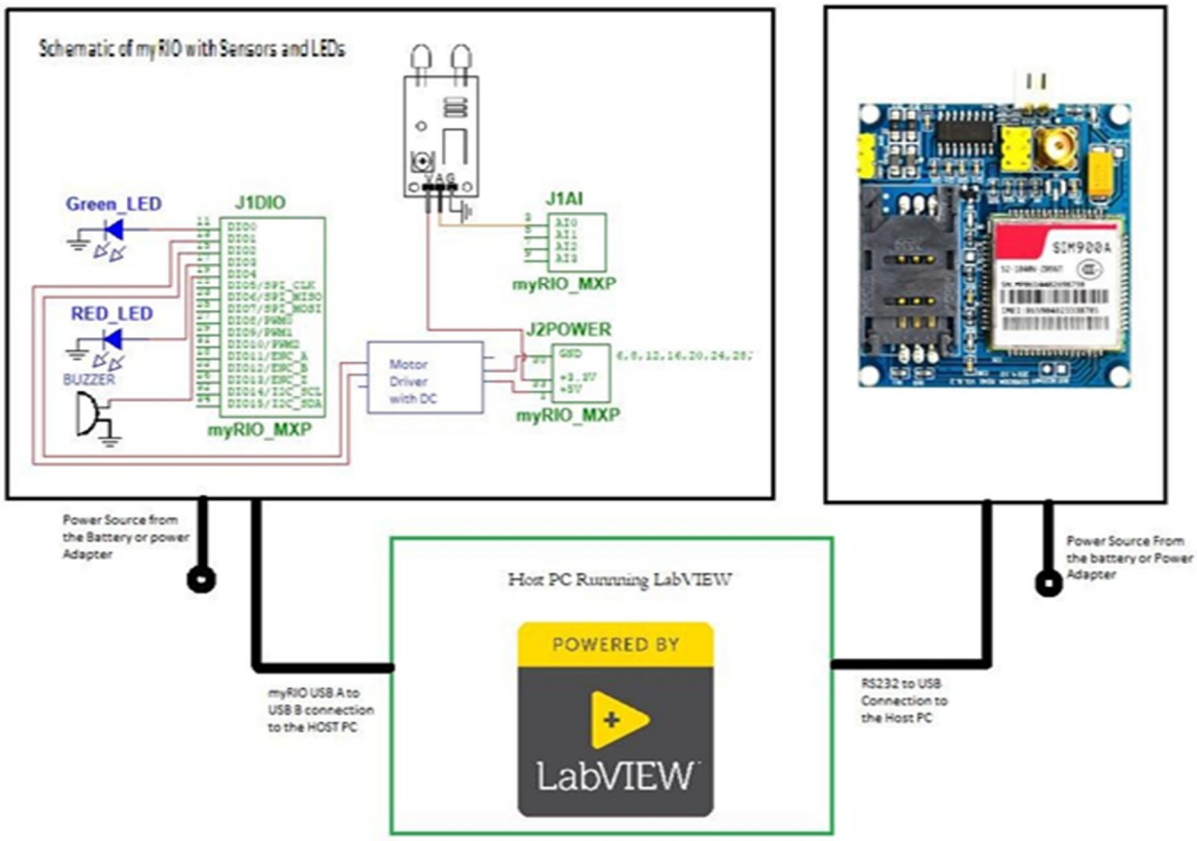


Fig.2 Schematic Diagram of the system

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

III. METHODOLOGY

Initially the process start to open the authentication system VI (Virtual Instruments) and choose COM port for GSM module. Then run the VI and wait for the signal from IR sensor. If the signal from the IR sensor is false, then it prints the statement "Please kindly approach nearby the sensor to get the authentication codes" and the same will be sent to the dweet platform. If the statement is true, it generates the OTP by entering into the True case of the case structure and enters the first frame of the flat sequence structure. Then a delay of 10s is provided for SMS to be sent .Now we have to enter the OTP in the secret pin control on the front panel, a delay of 10s is provided for the entering of OTP conveniently. The validate button on the front panel is pressed. In the next step, the entered secret pin is now verified with the OTP sent. The system checks if the secret pin is equal to the OTP sent.

If the secret pin is not equal to the OTP sent, then the authentication will be failed, the LED glows in RED. The system prints a statement "Validation Unsuccessful access denied". The buzzer also blows and the image at the time of transaction will be displayed and logged. After this process the system stop.

If the secret pin is equal to the OTP sent, then the authentication will be a success ,the LED glows in GREEN. The system prints a statement "Validation Successful access granted". The motor driver gets the command and drives the motor. and the image at the time of transaction will be displayed and logged. After this process the system stops. Fig. 3 shows the complete flow diagram of the proposed system.

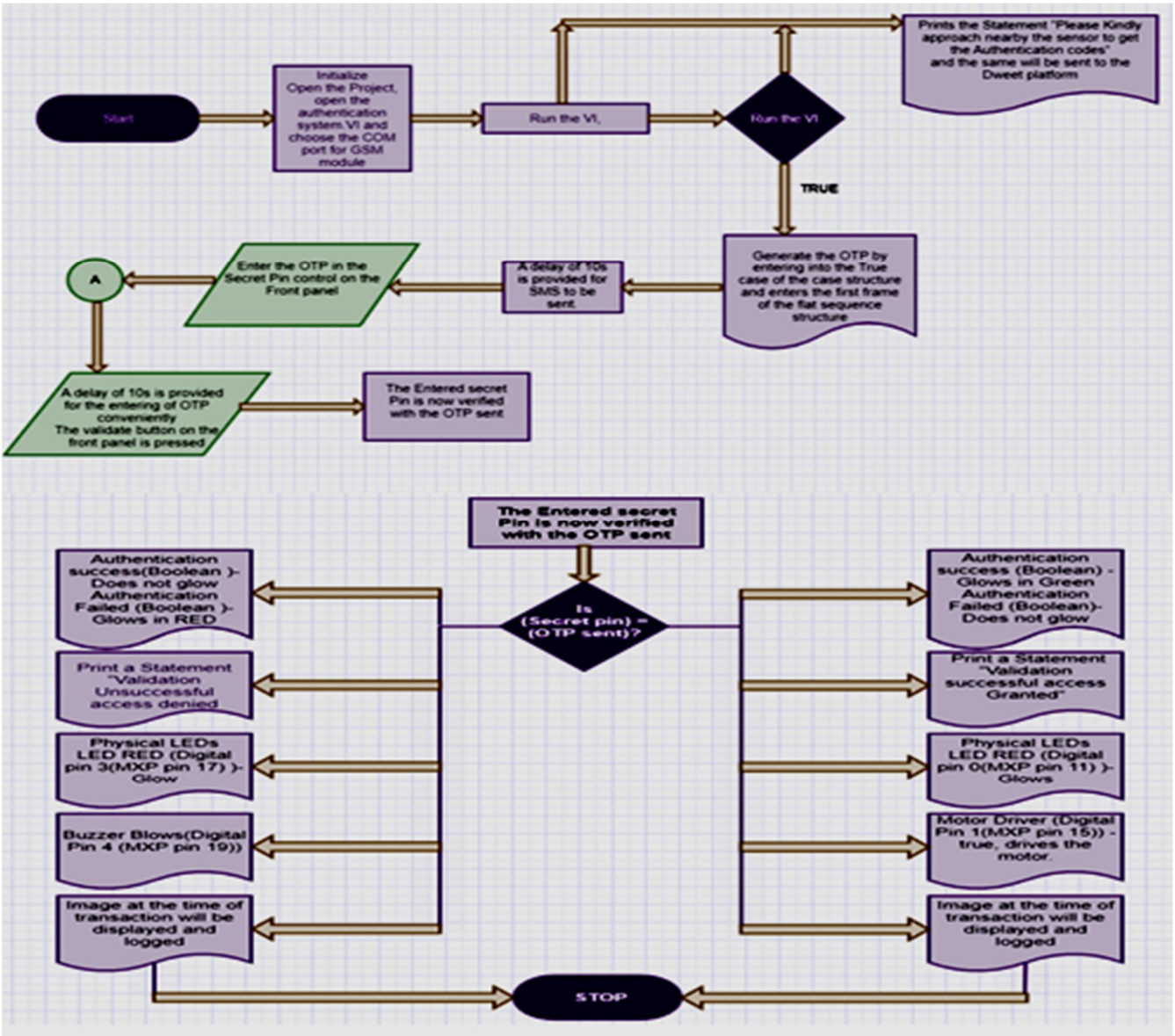


Fig.3 Flow Diagram

IV. IMPLEMENTATION AND RESULTS

A. Experimental Set up

The experimental setup consists of a flat cardboard box containing a NI myRIO embedded device, a GSM module as a subsystem and an infrared sensor for recognizing the person as shown in Fig.4. A camera is used for real-time images of the transaction and the LEDs, buzzer and the motor show the status of the transaction. Connections are made according to the schematic diagram.

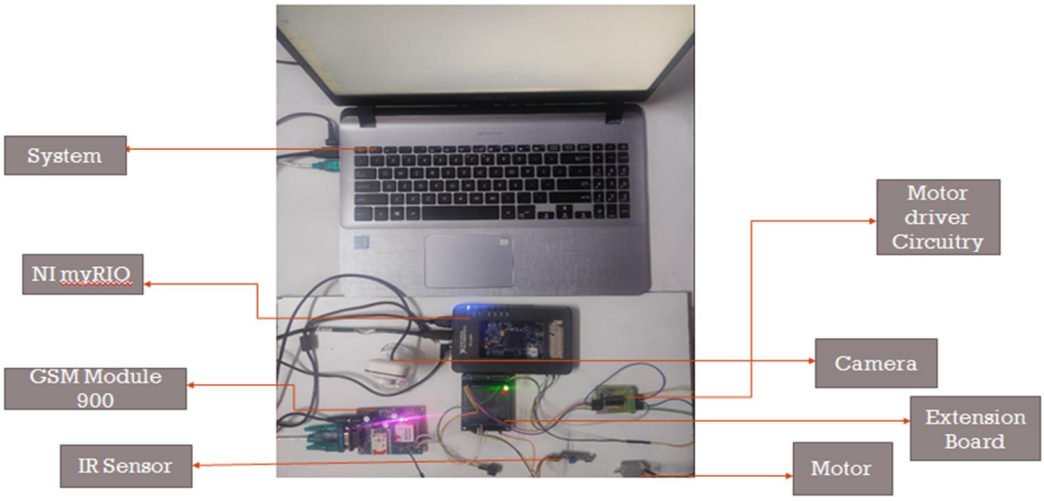


Fig.4 Experimental Setup

B. Implementation

Implementation of this work can be explained with the help of the LabVIEW code, which is divided into three parts, a main VI (Virtual Instruments) where Authentication based on coding.VI and two sub-VI; Send Sms.VI and Dweet Code.VI. A subVI corresponds to a subroutine in text based programming languages. “Send sms.vi” is the interfacing code used to order where each of the frames constitutes sending the command and receiving the feedback for communication with the GSM module. The GSM Module communication is done in a sequence. The entire code is divided into 11 frames of the Flat sequence structure. Each frame of code is dedicated to either initializing, writing commands or reading the byte data. The interfacing of the GSM module is done through the visa Serial driver of the LabVIEW software. Code for interfacing and sending the One Time Password (OTP) as shown in Fig 5. Authentication based on coding.VI is the main VI primarily divided into 2 cases of the outer case structure. The choices of the cases are governed by the output of the IR sensor. The true case of the case structure is chosen and the true case consists of a flat sequence structure which consists of 5 frames, which constitute a sequential execution of the code as shown in Fig 6.

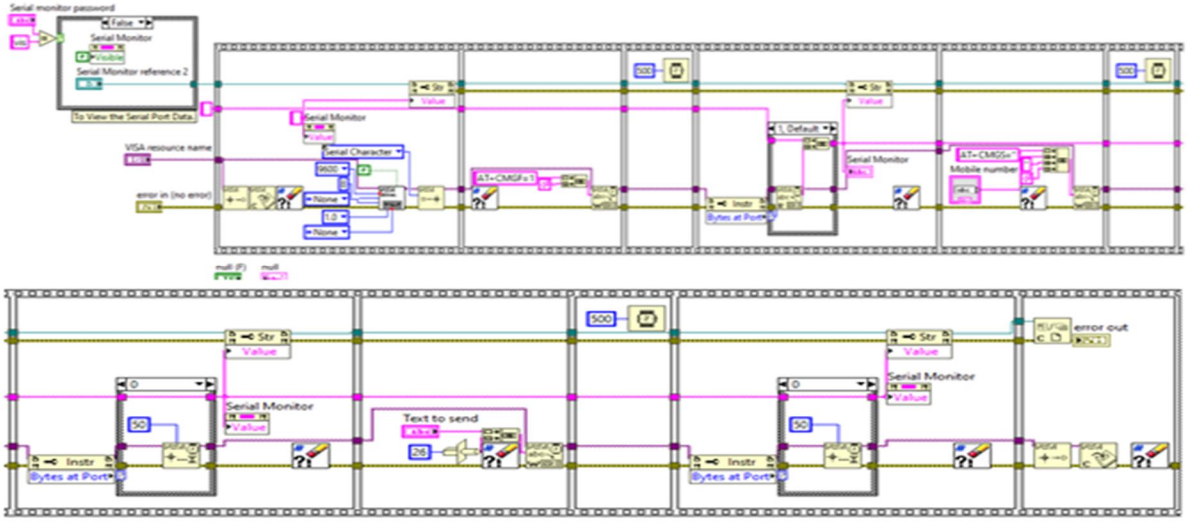


Fig.5 Lab VIEW code for interfacing and sending the OTP

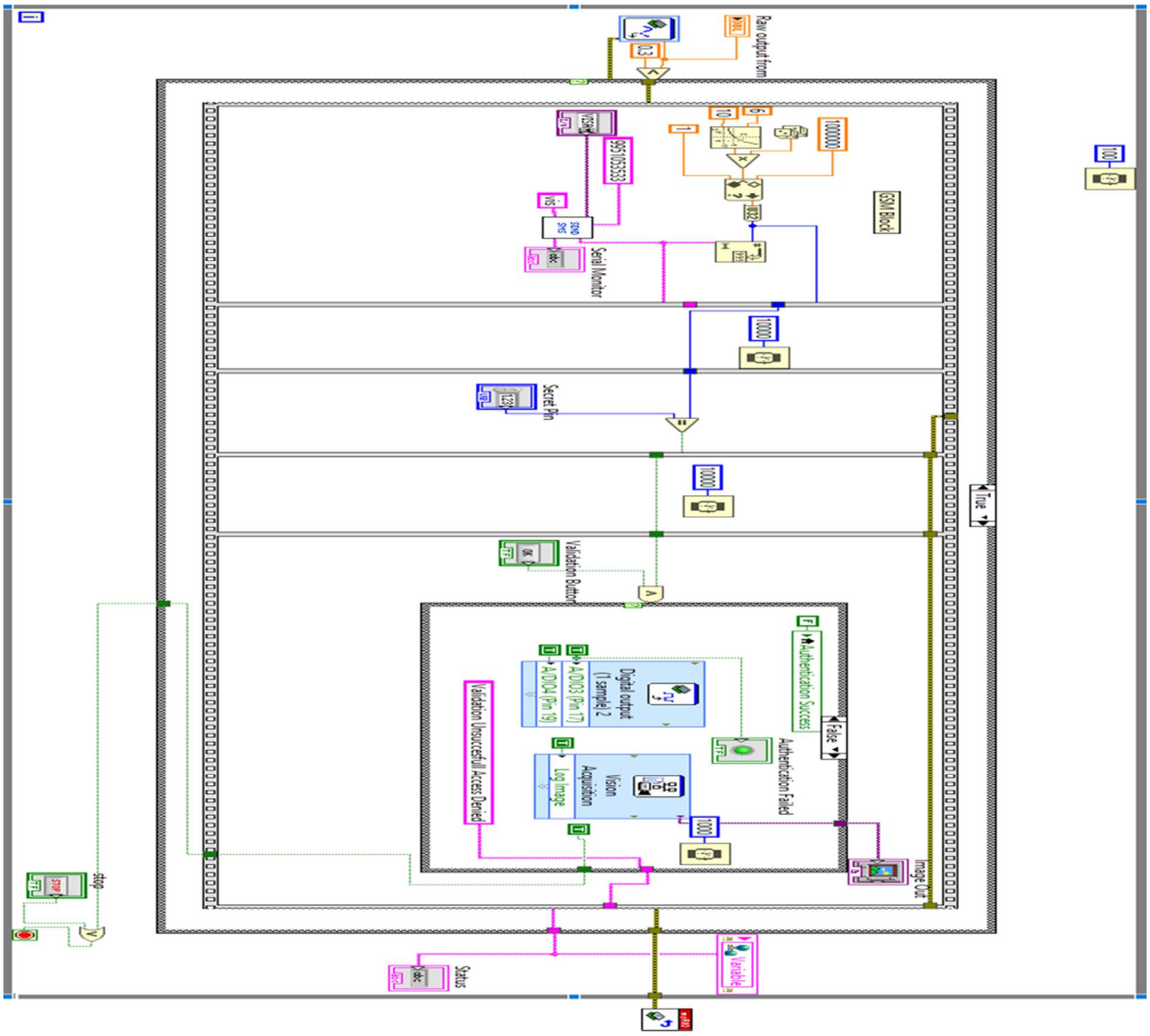


Fig 6. Lab VIEW Code for Authentication based code.vi

When the IR Sensor`s output is less than 0.3 V which indicates that a person is detected in front of the system. Therefore the VI is directed towards the true case and the first Frame of the flat sequence structure constitutes to the generation of the OTP and sending of the same, using the Send SMS.vi subVI which is used to interface with the GSM module. In Frame 2,10s delay is provided so that the OTP can be sent and received by the user In Frame 3 the user is allowed to enter the received OTP through the Secret pin Control on the Front Panel. and the entered OTP is compared with the generated OTP in the Frame 1.Then 0s delay is provided for the user to enter the OTP in Frame 4 Finally in Frame 5, based on the condition signal from the comparison of the secret pin with the generated OTP, followed by the pressing of the Validation button on the front panel, the case structure cases are chosen.

If the serect pin matches and the validation button is pressed, the true case is selected and the DIO Express VI supplies a real signal to the connected green LED, a true signal to the motor controller connected to the NI myRIO, which in turn results in DC current. Motor runs and shows axis movement If the secret pin does not match or the confirmation button is not pressed, the wrong case is selected and the vi express supplies a wrong signal to the green LED and a true signal to the red LED and the buzzer connected to the NI-Myrio. The replica LEDs on the front panels also receive the same signal as a hardware LED. In both cases, the transaction images are recorded on the device.

When IR Sensor is greater than 0.3v, the wrong case is chosen for the outer box structure and an instruction is printed on the front panel such as "Get closer to the nearby sensor and try again, which is then used to view the transaction details on the IoT- Upload platform. Dweet is an open source IoT platform used to share data via cloud storage.

C. Results and Discussion

Fig.7 shows the Authentication display status. After running the application , we enter the code which is sent through SMS and validate the code. If the code matches ,the green LED will glow and a message displayed as “Validation Successful. Access Granted” is displayed on the screen. Raw output from IR sensor is almost equal to 0, which means that there is an obstacle in front of the IR. When we enter an incorrect code, the red LED glows and the buzzer also blows up got message ”Validation unsuccessful Access denied.” is displayed on the screen. Fig. 8 shows the display of successful authentication and Fig. 9 shows the display of unsuccessful authentication.

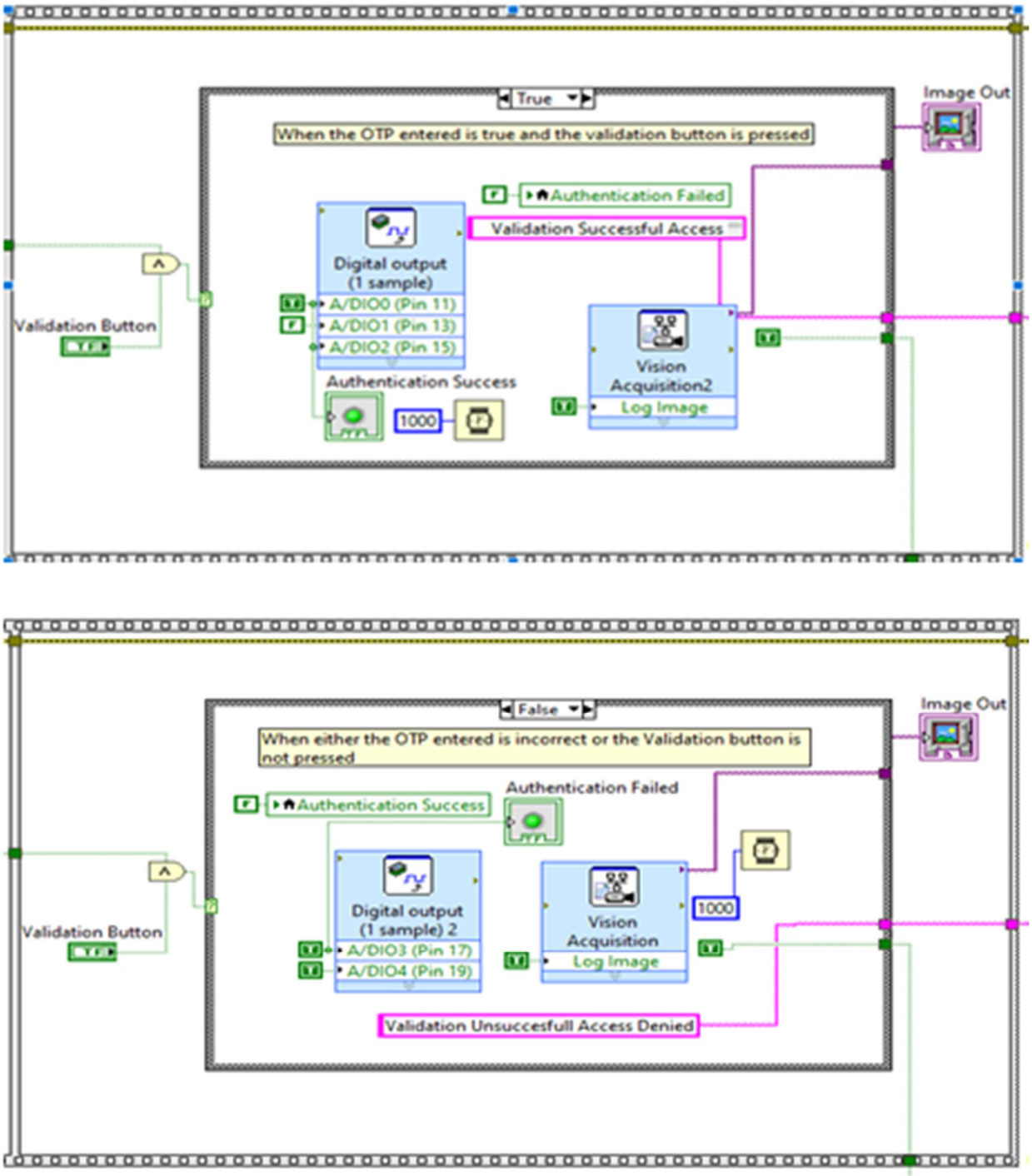


Fig7. Authentication and Display status

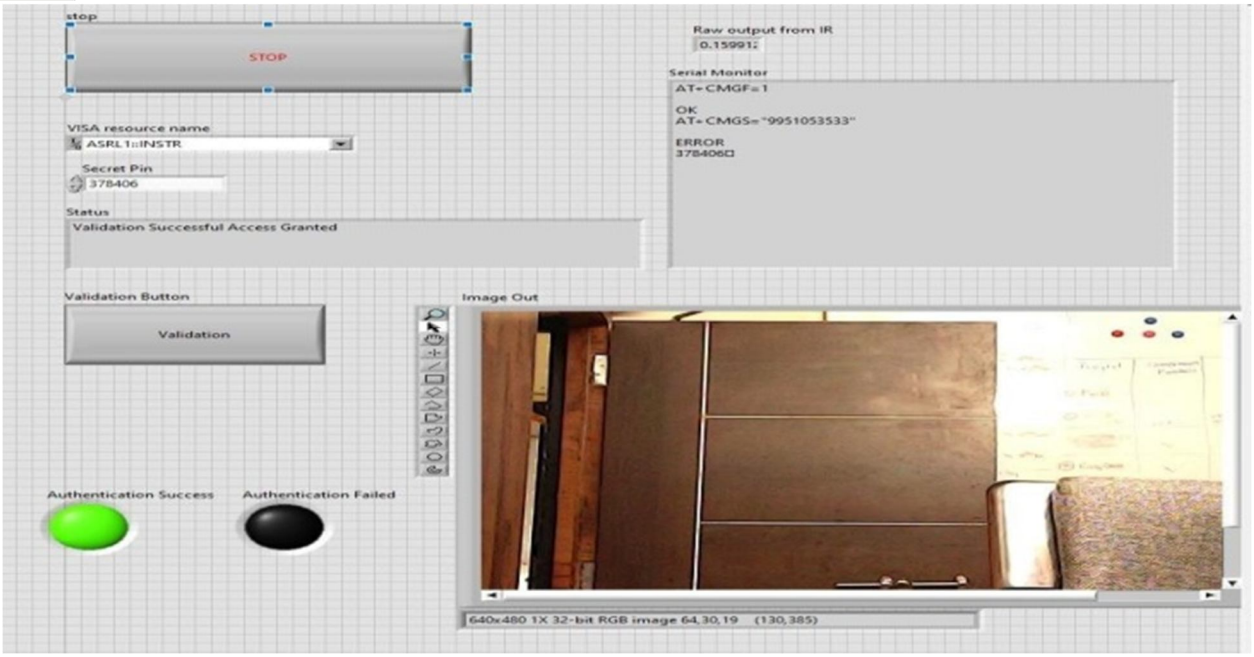


Fig.8 Successful Authentication

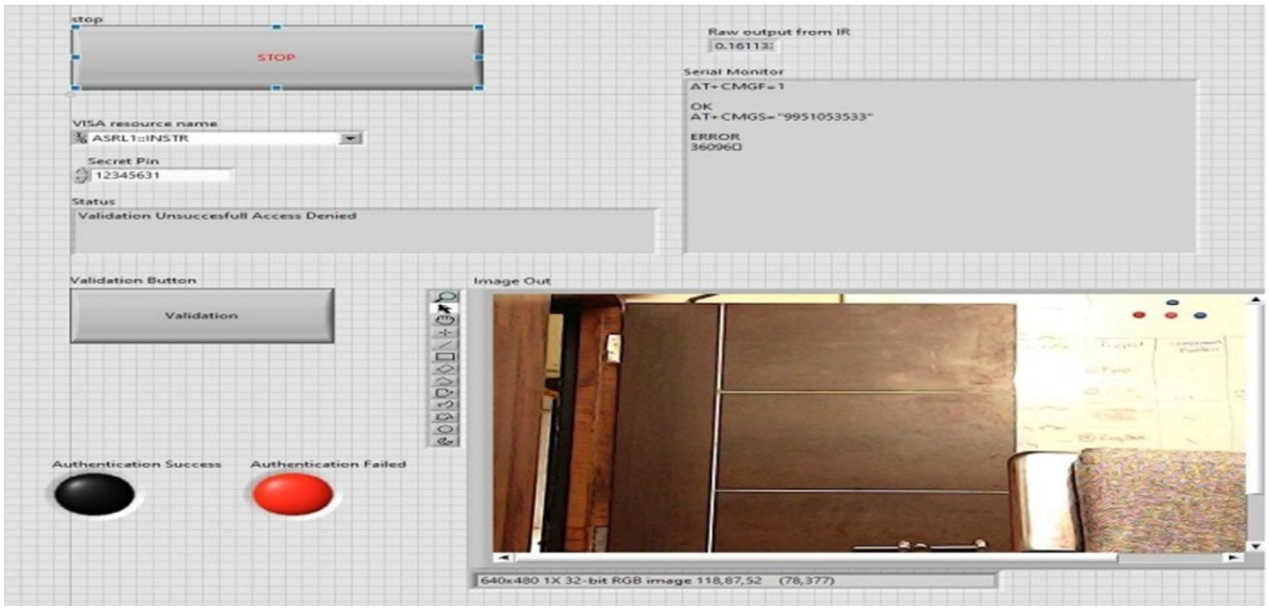


Fig.9 Unsuccessful Authentication

V. CONCLUSION

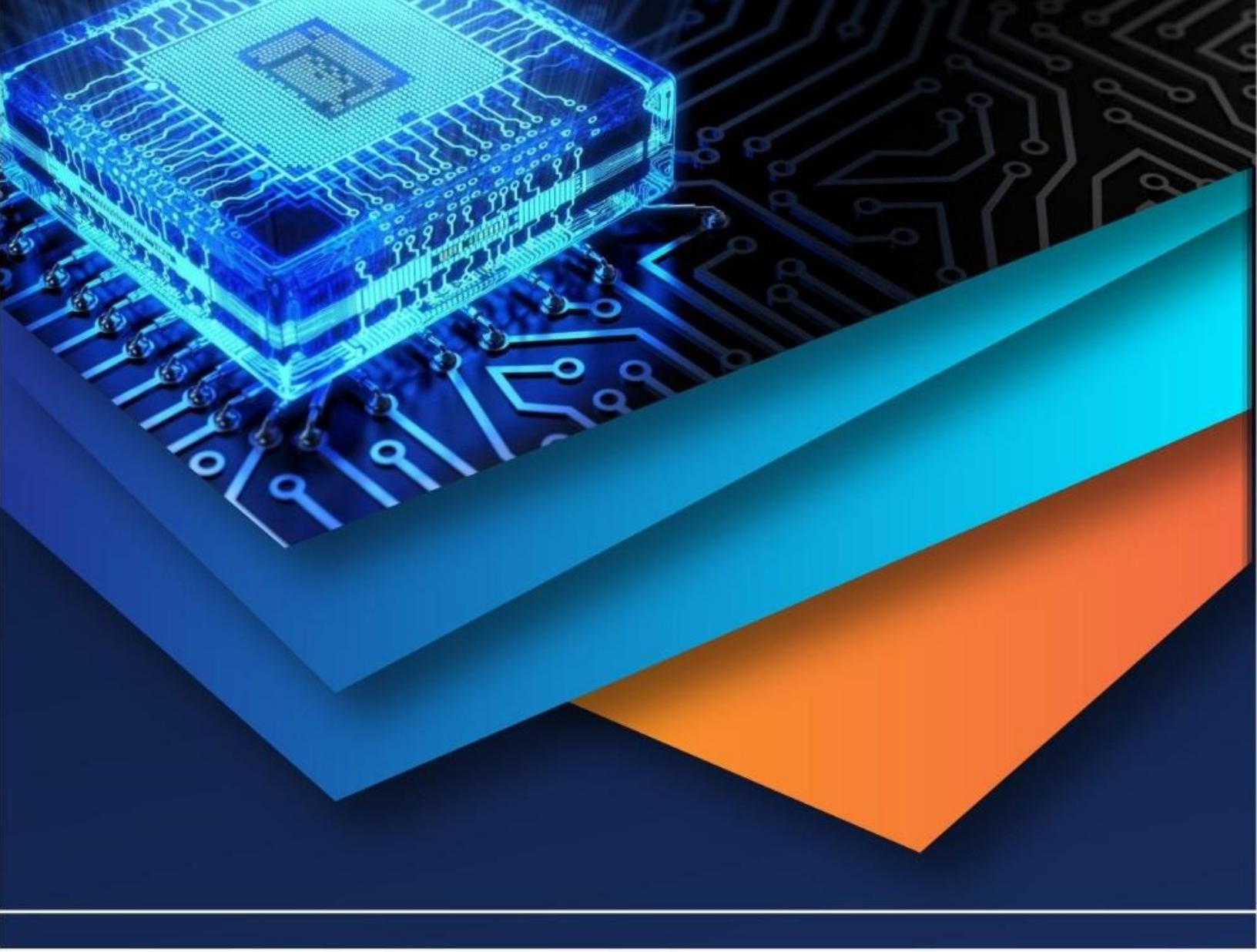
The proposed classified authentication system has been successful in improving security for the authentication systems. The authentication system developed using the LabVIEW Software and NI myRIO is a minimalistic approach towards a universal authentication system which can be implemented on any given system with minimal hardware changes. There are many future insights which shall make this concept more secure, more available and more essential on a daily basis. We have designed an IoT-based remote authentication digital door lock system using OTP. The authentication system is simple enough to use by physically challenged people without any struggle to move. This system allows single-person residents to relieve the anxiety caused by the password leakage and unforeseen visitors, making solve the growing social problems occurring in single person households. This system can also be applied to various sharing economy platforms such as lodging facilities and personal lockers.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

REFERENCES

[1] M. Becker, "Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy", Ethics and Information Technology, vol. 21, pp-307–317, 2019.
[2] P.Deeksha ,M.Gowri ,R.Sateesh ,M.Yashaswini and V.B.Ashika, " OTP Based Locking System using IOT", International Journal of Research Publication and Reviews, Vol..2,no.7,pp-352-356,2021.
[3] K. Rambabu, P. Aravind Sai, E. Samuel, P.N.V.S.M. Varma and M. Sumanth Reddy,"Monitoring and Controlling of Home Security System using IoT and LabVIEW", International Journal of Control and Automation , vol.913, no.4, pp- 596 – 605, 2020
[4] L.Kook, "Design and Implementation of a OTP based IoT digital door lock system and Applications", International Journal of Engineering research and Applications vol. 12, no.11,pp-1841-1846,2019.
[5] Krishna, Gopi & Kumar, P. & Ravi, K. & Sravanthi, M. & Likhitha, N.," Smart home authentication and security with IoT using face recognition", International Journal of Recent Technology and Engineering,vol. 7,pp- 705-709,2019..
[6] K. R Nadig , A. Kumar ,D.C. Mayuri , L.Pradeepand T. Somasekhar ," Secured Home Automation using OTP Authentication with Iot and Cloud Integration", International journal of Engineering Research & Technology, Vol.4, no.29 ,pp-1-4,2016.
[7] H.L. Wu , C.C. Chang , Y.Z. Zheng , L.S. Chen and C.C. Chen , "A Secure IoT-Based Authentication System in Cloud Computing Environment", MDPI Sensors, vol. 20,pp- 1-14,2020.
[8] K.Haribabu, S.V.S Prasad, M.S.Kumar ",An IOT based smart home automation using LabVIEW", Journal of Engineering and Applied Sciences,vol.13,no.6,pp-1421-1424,2018.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)