IJARSCT

ISSN (Online) 2581-9429

IJARSCT
Impact Factor: 6.252

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 2, Issue 2, July 2022

RAKSHA - The Smart Security System

Mr. Arun Kumbi[1], Mr. Kirankumar B K[2], Mr. Prasad S[3], Ms. Sahana S D[4] , Mr. Vishalkumar B[5]
Assistant Professor[1], Students[2,3,4,5]
Smt Kamala And Shri Venkappa M. Agadi College of Engineering and Technology, Laxmeshwar, India
arunk.cse@agadiengcollege.com, bkkirankumar123@gmail.com, prasadsalimath7@gmail.com,
sahanad0103@gmail.com, vishalkumarmb9380@gmail.com

Abstract: *Web-based technology has improved drastically in the past decade. As a result, security technology has become a major help to protect our daily life. In this project, we propose a robust security based on face recognition system with security for gas and fire. In particular, we develop this system to give access into a room for authenticated users and help us in the condition where there is LPG gas leak or fire catch. The classifier is trained by using a new adaptive learning method. The training data are initially collected from live images. The accuracy of the classifier is incrementally improved as the user starts using the system. A novel method has been introduced to improve the classifier model by human interaction and social media. By using a deep learning framework- TensorFlow, it will be easy to reuse the framework to adopt with many devices and applications. In addition to face Security system, we are going with Pin conformation, OTP and Finger print series.*

Keywords: Security System

I. INTRODUCTION

Access control is a security feature that controls how a user and the system communicate and interact with other systems and resources. Access control protects the system and resources from unauthorized access and can be a component that participates in determining the level of authorization after the authentication procedure is successfully completed [1]. Access control is an important requirement of any information system to protect data and resources against access and modification of data from unauthorized users [2].

Historically, the use of PINs, passwords, names, numbers, social security, and tokens has been widely used to verify that someone is recognized by the system. For example, the most commonly used is passwords. In its implementation, many passwords use the system to identify the correct password without knowing whether the password is used by the correct person. Different from the above problems, biometrics can offer prospects that closely link the authenticity of an individual person. The biometric system establishes a probabilistic assessment of a match which shows that the subject is the same as who the reference is stored [3]. One of the biometric factors that can be implemented is face recognition. Facial recognition is one of the pattern approaches for personal identification purposes in addition to other biometric approaches such as fingerprint recognition, signature, retina of the eye, and so on.The face is the one part of the human body that has a unique characteristics that can identify a person. Everyone has differences starting from the form of patterns and their own characteristics on the face [4]. Currently, the attacks of facial spoofing have always been considered a serious threat to the system. Facial spoofing attacks occur when someone tries to impersonate another person by faking a face and thus the attacker gains unauthorized access and benefits [5]. Primarily 3D masks which basically can fool the system and even humans. To overcome the most common spoofing attacks is to apply other authentication factors using the One Time Password (OTP) code. OTP is a one-time password that cannot be used a second time [6]. By registering a mobile number in the system and whenever the user accesses the system, the system will send a one-time access code (OTP) via SMS which ensures that a legitimate user has requested access to the service [7].

There are many access control system applications available on the market. However, creating our own access control system can of course set our own desired security model. Furthermore, we can avoid the pitfalls that system builders might set if we buy an existing control system. To that end, in this project, we implemented four-factor authentication on the access control prototype for our own need. The authentication factors used are face recognition as the first

DOI: 10.48175/IJARSCT-5843

authentication factor, pin code as its second authentication factor, series finger print verification as its third authentication factor and OTP SMS-Tokens as the four authentication factor.

II. OBJECTIVES

- Creating a **SECURE ROOM** framework where we protect from LPG gas leak, fire catch and unauthorized person.
- Make a **Device** which can identify gas leak as well as fire catch and alert message to fire fighters.
- Make a **Security Authorization System** which includes Face recognition, Password verification, OTP verification and Fingerprint with sequential verification.
- To provide a **Smart Monitoring System** anywhere in the world.

Control for Security

In this research, the security system offer an effective feature which are intrusion detection and fire detection. This system can be able to notify the authority as well as the security officers based on the occurrences.

Intruder Detection

As we can see in figure 1, if any intruder is detected by the motion sensor/reed sensor/laser sensor, the system will immediately notify the nearby police station as well as the authority.

Fire Detection

As we can see in figure 1, if the MQ2 Gas module sense gas/smoke/fire, the system will be able to notify nearby fire service as well as the authority.

Arduino(Mega2560)

In Figure 2 the Arduino Mega is the driver behind our entire project, not only does it receive and interpret signals from our sensor devices, but it also allowed us to run the program to the system by any mistakes we could potentially make in connections. The Mega is affordable at roughly sixty dollars.

Smoke Sensor(MQ2)

In Figure 3 the MQ-2 Gas Sensor module is useful for gas leakage detecting in home and industry. It can detect LPG, i-butane, propane, methane, alcohol, hydrogen and smoke.

III. PROPOSED METHODOLOGY

In the below figure, the main objective is to provide security for room and offices. There are security systems which depends on face recognition. In this system we are adding some more features to make system more accurate. We will be having fingerprint scanner, Pin code and OTP verification.

Starting of this project, we will train a face recognition system which can recognise authorised person. This will be done by using deep learning models. This deep learning model will be trained in a such a way that it can accurately recognise a person. Fixing a web camera on the door and live video input of this web camera will be fed to a CNN model to recognise the person in front of the door. If the person is recognized correctly, then we will go to the next process. If the person is not recognized than we will send a message to user as well as a police officer. If the person is recognized in the web camera he will be asked to enter the pin code. If the pin code has been entered in the right form, then the person will be asked to enter the OTP sent to his registered mobile number. If pin code and OTP has been entered in a reverse order then a message will be sent to police officer as well as home

In the above fig 1, the main objective is to provide security for room and offices. There are security systems which depends on face recognition. In this system we are adding some more features to make system more accurate. We will be having fingerprint scanner, Pin code and OTP verification.

Starting of this project, we will train a face recognition system which can recognize authorized person. This will be done by using deep learning models. This deep learning model will be trained in a such a way that it can accurately recognize a person. Fixing a web camera on the door and live video input of this web camera will be fed to a CNN model to recognize the person in front of the door.

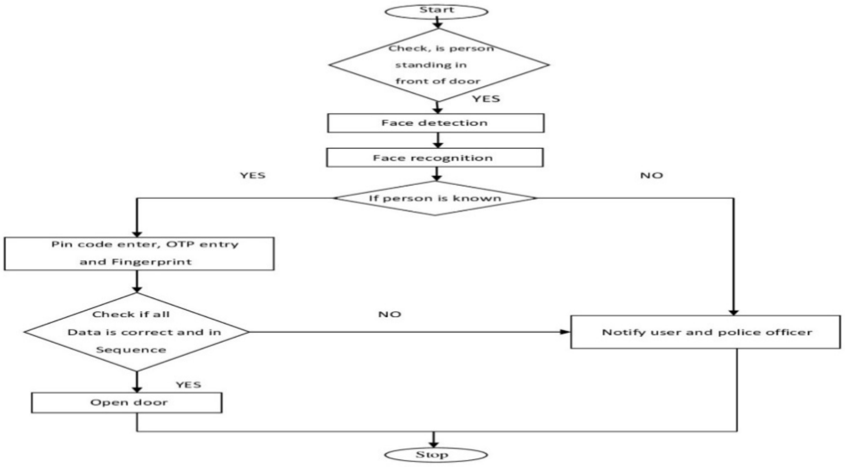
Start
Check, is person standing in front of door
YES
Face detection
Face recognition
YES
NO
If person is known
Pin code enter, OTP entry and Fingerprint
Check if all Data is correct and in Sequence
NO
Notify user and police officer
YES
Open door
Stop

Figure 1 Flow Chart of Security System

If the person is recognized correctly, then we will go to the next process. If the person is not recognized than we will send a message to user as well as a police officer. If the person is recognized in the web camera he will be asked to enter the pin code. If the pin code has been entered in the right form, then the person will be asked to enter the OTP sent to his registered mobile number. If pin code and OTP has been entered in a reverse order then a message will be sent to police officer as well as home owner.

Once the person has been verified from face recognition, pin code and OTP verification; The user is informed to enter three fingerprints. If these fingerprints are entered in right sequence the user will be allowed to access the system or the door will be unlocked. If the person enters fingerprint in wrong sequence or in reverse order then again a message will be sent to owner and police officer.

IV. WORKING

The authentication factors used are face recognition as the first authentication factor, pin code as its second authentication factor, series finger print verification as its third authentication factor and OTP SMS-Tokens as the four-authentication factor.

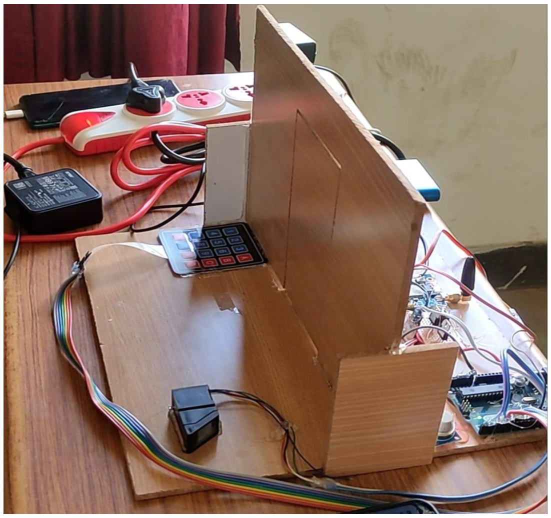

Figure2: View of the System.

DOI: 10.48175/IJARSCT-5843

The main objective is to provide security for room and offices. There are security systems which depends on face recognition. In this system we are adding some more features to make system more accurate. We will be having OTP Generation, OTP verification and Fingerprint sensor for Fingerprint sequence Entry.

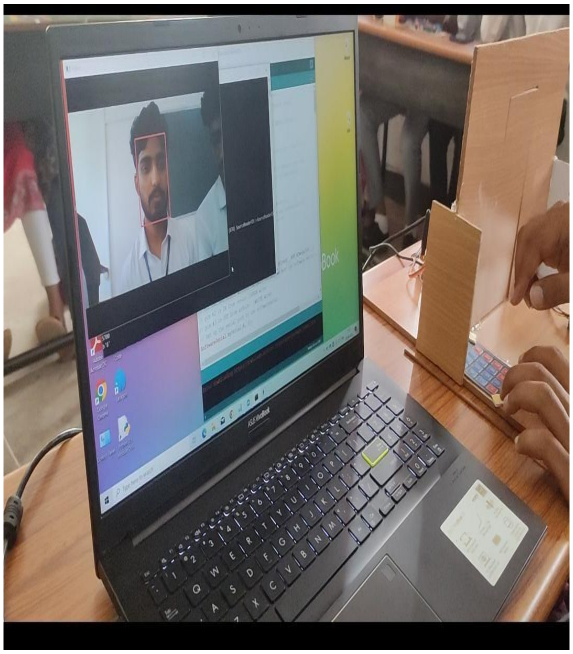

Figure3: Web camera Processed.

Starting of this project, we will train a face recognition system which can recognise authorised person. This will be done by using deep learning models. This deep learning model will be trained in a such a way that it can accurately recognise a person. Fixing a web camera on the door and live video input of this web camera will be fed to a CNN model to recognise the person in front of the door.

If the person is recognized correctly, then we will go to the next process. If the person is not recognized than we will send a message to user as well as a police officer. If the person is recognized in the web camera, He will be asked to enter the OTP as pin code. The OTP is sent to his registered mobile number. If OTP has been entered in a correct order then the door will be open. If OTP has been entered in a reverse order then a message will be sent to police officer as well as home owner.

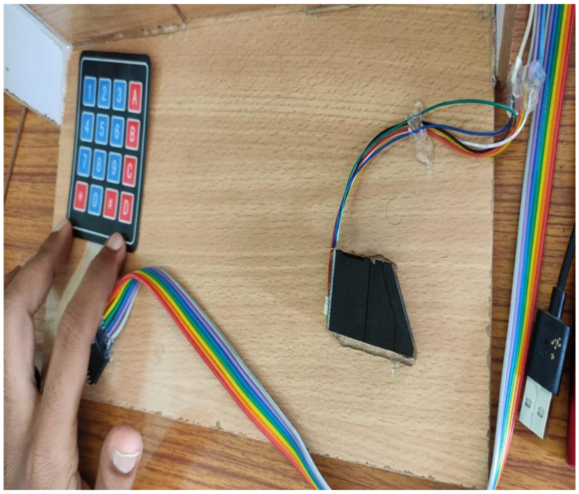

Figure 4: Front View of Door.

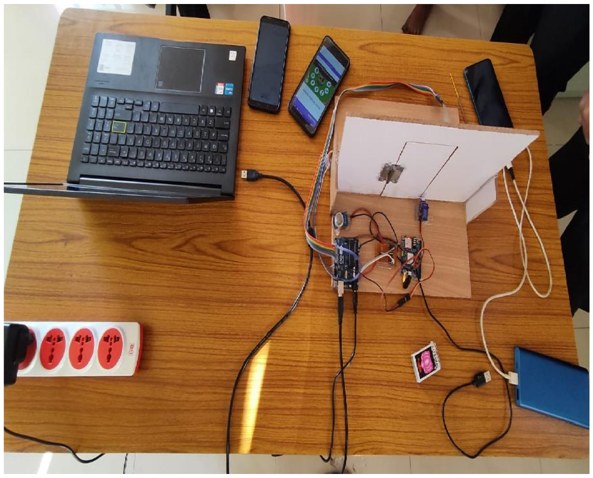

Figure 5: Top View of System

Infront of the door, to enter the OTP received: the Keypad is placed at the left side of the door in the system. To enter the sequence of the Fingerprint Series: Fingerprint Sensor is placed at the right corner of the door in the system.

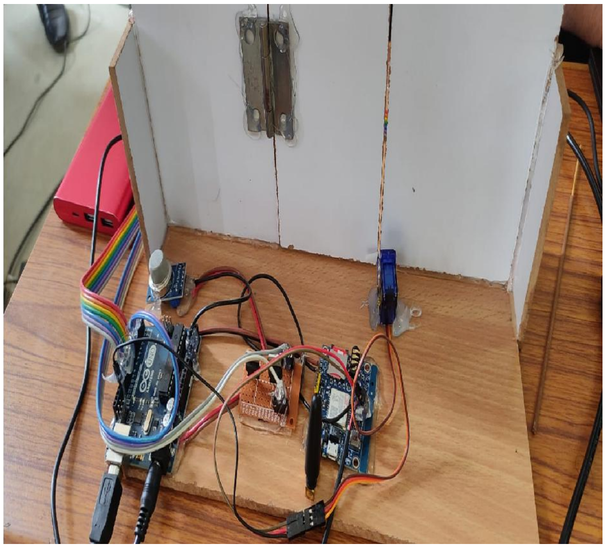

Figure 6: Backside View of Door.

- Arduino Uno: it is a microcontroller which controls and handles all the devices connected to the system and it is placed behind the door,
- GSM Model: used to communicate with mobile telephone network. This uses SIM to identify their device to the network,
- Servo Motor: Attached at the back of the door which act as the DOOR LOCKER.

If this turns straight; door unlocks.

Once the person has been verified from face recognition, pin code and OTP verification; The user is informed to enter three fingerprints. If these fingerprints are entered in right sequence the user will be allowed to access the system or the door will be unlocked. If the person enters fingerprint in wrong sequence or in reverse order then again a message will be sent to owner and police officer.

V. RESULTS

1. Created **IoT kit** which can detect fire catch and gas leak using sensors.
2. Once there is a fire catch or gas leak then notifying the owner and nearby firefighters.

DOI: 10.48175/IJARSCT-5843

3. Made a **Authorization System** which has four verification factors such as Face recognition, OTP verification Password verification and fingerprint series verification.
4. If **Unauthorized person** is trying to access the system then it will notify the owner as well as nearby police station.
5. **Reverse Entry** of password and fingerprint sequence will automatically inform the nearby police station.

VI. CONCLUSION

There are many authentication schemes in the current state. Some of them are based on user's physical and behavioral properties, and some other authentication schemes are based on user's knowledge such as textual and graphical passwords. Moreover, there are some other important authentication schemes that are based on what you have, such as smart cards. Among the various authentication schemes, textual password and token-based schemes, or the combination of both, are commonly applied.

However, as mentioned before, both authentication schemes are vulnerable to certain attacks. Moreover, there are many authentication schemes that are currently under study and they may require additional time and effort to be applicable for commercial use.

The Smart Security System is a multifactor authentication scheme that combines these various authentication schemes into a single system environment. The choice of what authentication schemes will be part of the user's fingerprint and OTP sent to his mobile number. This reflects the user's preferences and requirements.

Suppose a person is standing in front of the door and the owner wants to give access to this person, owner can do this by using a Android app and unlocking the door.

REFERENCES

[1]. X. Geng, Z. Zhou and K. Smith-Miles, "Individual Stable Space: An Approach to Face Recognition Under Uncontrolled Conditions," in IEEE Transactions on Neural Networks, vol. 19, no. 8, pp. 1354-1368,Aug.2008, doi:10.1109/TNN.2008.2000275.

[2]. Y. Wang and J. Su, "Symmetry description and face recognition using face symmetry based on local binary pattern feature," Proceedings of the 32nd Chinese Control Conference, Xi'an, 2013, pp. 3955-3960.

[3]. Wicaksono, M F., & Rahmatya, M D. (2020). Implementasi Arduino dan ESP32 CAM untuk Smart Home. Jurnal Teknologi dan Informasi (JATI) Volume 10 No. 1 March Edition 2020, P-ISSM 2088-2270, EISSN 2655-6839.

[4]. Setiawan, Andi., & Purnamasari, Irma, Ade. (2010). Pengembangan Passive Infrared Sensor (PIR) HC-SR501 dengan Microcontrollers ESP32-CAM Berbasis Internet of Things (IoT) dan Smart Home sebagai Deteksi Gerak untuk Keamanan Perumahan. Prosiding Seminar Nasional Sisfotek Vol.3 No.1 2019 ISSN 2597-3584.

[5]. Ai-Thingker Technology Co, "ESP32-CAM Wi-Fi+BT SoC Module v1.0, Shenzhen 2017. Kale, Archita. Dhawan, Utkarsh. (2016). TOTP Based 2-Factor Authentication: Future of Security. Imperial Hournal of Interdisciplinary Research (IJIR) Vol. 2 Issue. 10, 2016.

[6]. Akshay v. Bhoyar, Shruti A. Borgave, A.S Bhandare. 2014. "Wireless Fingerprint Based Attendance System Using Zigbee Technology", International Journal of Innovative Resarch In Technology, ISSN: 2349-6002,Volume 1, Issue 11.

[7]. Ravishankar Yadav, Sumita Nainan.2014. "Design of RFID Based Student Attendance System with Notification to Parents Using GSM", International journal of Engineering Research & Technology (IJERT) ,ISSN:2278-0181, Vol.3

DOI: 10.48175/IJARSCT-5843