

AI BASED VERIFICATION SYSTEM USING RASPBERRY PI

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering in Mechatronics

by

DEEPAK JEFFERSON (Reg.No-39090008)

VIGNESH S (Reg.No-39090061)



**DEPARTMENT OF MECHATRONICS
SCHOOL OF MECHANICAL ENGINEERING**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

**Accredited with Grade "A" by NACC | 12B Status by UGC | Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600119**

MAY - 2023



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NACC | 12B Status by UGC | Approved by AICTE

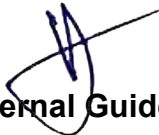
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600119

www.sathyabama.ac.in

DEPARTMENT OF MECHATRONICS

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **DEEPAK JEFFERSON (39090008), VIGNESH S (39090061)** who carried out the Project entitled "**AI BASED VERIFICATION SYSTEM USING RASPBERRY PI**" under our supervision from Jun 2022 to May 2023.



Internal Guide

Mr. V JAYAPRAKASH, M.Tech., MIE., (Ph.D.),



Head of the Department

Dr. S. PRAKASH, M.E., Ph.D.,

Submitted for Viva Voice Examination held on 10 May 2023



Internal Examiner



External Examiner

DECLARATION

We **DEEPAK JEFFERSON (39090008)** and **VIGNESH S (39090061)** hereby declare that the Project Report entitled “**AI BASED VERIFICATION SYSTEM USING RASPBERRY PI**” done by us under the guidance of **Mr. V JAYAPRAKASH, M.Tech., MIE., (Ph.D.)**, at **SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Mechatronics.

1)



DATE:

PLACE: CHENNAI

2)



SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

We are pleased to acknowledge our sincere thanks to the **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. We are grateful to them.

We convey our thanks to **Dr. S. PRAKASH, M.E., Ph.D.**, Dean, School of Mechanical engineering and Head of the Department, Department of Mechatronics for providing us necessary support and details at the right time during the progressive reviews.

We would like to express our sincere and deep sense of gratitude to our Project Guide **Mr. V. JAYAPRAKASH, M.Tech., MIE., (Ph.D.)**, for his valuable guidance, suggestions and constant encouragement paved the way for the successful completion of our project work.

We wish to express our thanks to all Teaching and Non-teaching staff members of the Department of Mechatronics who are helpful in many ways for the completion of the project.

ABSTRACT

In today's world, many things require a minimal age category. People aren't allowed to certain things/places if they don't pass the age test. For example, driver's license, entering into a pub/bar/tasmac, entering into porn websites, etc. But people who do not pass the age test are also doing things that they are not allowed to do because the age verification test is not done right. Because of this, these individuals are learning new bad habits and getting addicted to them. It is not safe and good for them and as-well-as for the community. So, it is, therefore, necessary that we adopt some measures to minimize this practice. So, we hereby propose an efficient and reliable solution. Here in this project, we are creating an age verification and authorization system using Raspberry Pi through GOVT ID. The system uses a Raspberry-pi micro-controller. It consists of two cameras, one for face recognition and another one for capturing the ID proof.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE NO
	ABSTRACT	I
	LIST OF FIGURES	III
	LIST OF ABBREVIATION	IV
1	INTRODUCTION	1
2	LITERATURE SURVEY	3
3	AIM AND SCOPE OF THE PRESENT INVESTIGATION	9
	3.1 AIM	9
	3.2 SCOPE OF THIS PROJECT	10
4	EXPERIMENTAL SETUP AND METHODOLOGY	13
	4.1 EXPERIMENTAL SETUP	13
	4.2 METHODOLOGY	13
	4.3 MATERIALS AND COMPONENTS	16
	4.4 PROGRAM CODE	19
5	RESULTS AND DISCUSSION, PERFORMANCE ANALYSIS	29
	5.1 RESULTS AND DISCUSSION	29
	5.2 PERFORMANCE ANALYSIS	30
6	SUMMARY	35
	CONCLUSIONS	36
	REFERENCES	37

LIST OF FIGURES

FIGURE NO	TITLE NAME	PAGE NO
4.1	EXPERIMENTAL SETUP	13
4.2	FLOW CHART	14
4.3	BLOCK DIAGRAM	15
4.4	RASPBERRY-PI	16
4.5	CAMERA	17
4.6	TOUCHSCREEN DISPLAY	18
4.7	SPEAKERS	19
5.1	READING AADHAR CARD NUMBER	31
5.2	CAPCHA RECOGNIZATION IS DONE	32
5.3	OTP ENTERED	33
5.4	THE DETAILS EXTRACTED FROM THE AADHAR WEBSITE	34

LIST OF ABBREVIATION

S.NO	ABBREVIATION	MEANING
1	RFID	RADIO FRQUENCY IDENTIFICATION
2	IOT	INTERNET OF THINGS
3	FDA	FOOD AND DRUG ADMINISTRATION
4	PCA	PRINCIPLE COMPONENT ANALYSIS
5	LDA	LINEAR DISCRIMINATE ANALYSIS
6	ICA	INDEPENDENT COMPONENT ANALYSIS
7	SVM	SUPPORT VECTOR MACHINE
8	PACS	PICTURE ARCHIVING AND COMMUNICATION SYSTEM
9	GPIO	GENRAL INPUT OUTPUT
11	URL	UNIFORM RESOURCE LOCATOR
12	HTML	HYPERTEXT MARKUP LANGUAGE
13	JSON	JAVASCRIPT OBJECT NOTATION
14	DOM	THE DOCUMENT OBJECT MODEL
15	KNN	K-NEAREST NEIGHBOURS

CHAPTER 1

INTRODUCTION

Security is extremely important in our lives because it guarantees that people and property are kept secure and in good shape. Security systems are systems that are used to ensure the safety of people and property. These systems prevent unauthorized personnel from gaining access to secured physical or intellectual property. One of the major reasons for theft is unauthorized persons having access to our property. And also the number of access credentials theft is increasing. Losing our property or information or anything in such a way pains because we have spent so many months of hard work in our job to earn

Face detection systems are becoming increasingly popular since they are more secure than fingerprint readers and inputted passwords. You may have noticed that your smartphone has a face unlock feature that makes things incredibly simple. Face detection is also utilised for surveillance in various places, including airports, train stations. As a surveillance system, we will create a Face Recognition system on Raspberry Pi with the OpenCV Library. This system has been thoroughly tested by me and will undoubtedly function correctly.

It, like any other Identification of Faces system, is made up of a pair of Python scripts, one of which functions as a training programme that analyses a series of photographs of a certain person and generates the data set (YML File) from it.

The Recognizer is the second application, which recognises a face and then uses this YML file to recognise the face in order to proclaim the person's name. The software on this page are intended for use with the Raspberry Pi (Linux).

Face recognition looks to give the greatest mix of accuracy and user participation among various biometrics. As a result, face recognition has shown to be the most effective method for access control applications in settings that do not require high security, such as offices and businesses. Despite achieving over 90% accuracy in controlled circumstances, 2D face recognition algorithms continue to suffer from poor performance due to variable operating variables such as illumination variations, location changes, and facial expressions.

By assessing facial geometry rather than light intensity, 3D face recognition can increase resilience in varied illumination, position change, and

facial expression situations. Furthermore, because facial surface information is used rather than 2D images, the 3D approach is more difficult to create. Several studies are presently being undertaken on the use of 3D facial recognition in access control systems. The outcomes of the study are largely concerned with data preparation, analysis, and categorization of 3D face features.

CHAPTER 2

LITERATURE SURVEY

Aastha "Security of Radio Frequency Identification Technology" Advance in computational science and technology ISSN: 0973-6107, Vol: 10, pp. 2427-2433, Aug 2017.

This paper presents the introduction to the expected security mechanisms required to boost security of RFID. This study is related to key benefits of RFID. The future security mechanism for the improvement of RFID.

Becker, C. 2004. A new game of leapfrog? Modern Healthcare 34 (28): 38.

The focus of this article is to review and analyse the impact of privacy issues in RFID adoption in the healthcare domain, as well as to present a conceptual framework for analysing the relationship between technology and regulations in light of the Fair Information Practise (FIP) principles to ensure patients' privacy. Our conceptual framework examines the design of Privacy Enhancing Technologies (PETs) and analyses existing rules to identify compliance challenges using the FIP principles as a guideline.

Brewin, B. 2004. FDA backs RFID tags for tracking prescription drugs. Computerworld 38 (8): 4.

This paper talks about an RFID~based application in an assistive environment called "Smart Drawer", which tracks medicine taking for the elderly. We investigate the hardware involved to build such an application and we develop the software infrastructure to create a functional system to assist patients and care givers with the medication procedures and also collect data for future use.

N. Chilamkurti, S. Zeadally, and H. Chaouchi, Next-Generation Wireless Technologies (4G and beyond). 2013.

This paper discusses about technological revolution is the result of the emergence and evolution of a wide variety of new wireless networking technologies. Now people using these technologies are able to access the network and control many applications at will with their handheld devices anywhere, anytime. Although these technologies have made a long lasting impact in the revolution, it has also opened

up various challenging issues which are yet to be resolved to make them more efficient and cost-effective. Wireless technologies are used in mobile cellular networks, wireless access network, Mobile Adhoc Networks (MANET), Wireless Sensor Networks (WSNs), Wireless Mesh Networks (WMNs), Vehicular Adhoc Networks (VANETs) and more recently Internet of Things networks.

B. Cui, T. Xue, “Design and realization of an intelligent access control system based on voice recognition”, Proc. of International Colloquium on Computing, Communication, Control, and Management, pp. 229-232, 2001.

The speech recognition arithmetic theory examines the pretreatment of voice signals, character distillation, and pattern matching. The experiment findings show that the system capacity is stable and the identification is effective.

Davinder parkash, Twinkle Kundu, Kreet Kaur” the RFID technology and its applications: a review” International Journal of Electronics, Communication & Instrumentation Engineering Research and Development (IJEIERD) ISSN 2249-684X Vol.2, Issue 3 Sep 2012 109-120

The goal of this study is to go through RFID technology and its applications. This document provides a quick overview of RFID principles, RFID tag and reader categorization, frequency utilised, and current applications.

Glabman, M. 2004. Room for tracking: RFID technology finds the way. Materials Management in Health Care, May, 26–38.

In this paper we discuss the potential benefits, the areas of applications, implementation challenges and corresponding strategies of RFID in the healthcare.

K. S. Huang and S. M. Tang, “RFID applications strategy and deployment in bike renting system,” in Proc. ICACT 2008, pp. 660-663 [20]

This paper considered a strategy and a process in bike renting, and then designed a structure of RFID. Finally provide an approach to reference

**Hansung Lee, Soo-Hee Park, Jang-Hee Yoo, Se-Hoon Jung, Jun-Ho Huh
“Face Recognition at a Distance for a stand alone Access Control System”
Multidisciplinary Digital Publishing Institute, Vol. 20, Jan 2020**

This paper presents the design and implementation Of a user-friendly, stand-alone access control system based on human face recognition at a distance. The local binary pattern (LBP)-AdaBoost framework was employed for face and eyes detection, Which is fast and invariant to illumination changes.

F. Lourenco and C. Almeida, “RFID based monitoring and access control system,” in Proc. INFORUM, 2009

This study outlines the design of an RFID-based security and access control system for use at Punjab University dorms. To do the desired duty, the system integrates RFID technology with biometrics. When the RFID scanner at the hostel's door identifies a number, the system records the user's photograph and searches the database for a match. Access is given if both the card and the taken image correspond to a registered user; otherwise, the system activates the alarm and sends an emergency call to the security van via GSM modem. This manner, suspicious individuals can be identified.

X. L. Meng, Z. W. Song, and X. Y. Li, “RFID-Based security authentication system based on a novel face-recognition structure,” in Proc. WASE International Conference on Information Engineering, 2010, pp. 97-100.

RFID-based systems are discussed in this study. Door access control with Arduino is based on a security access and control system that makes use of RFID and Arduino. RFID embedded chips use radio waves to gather and read data from objects. Barcode labels have been in use for more than 30 years, however emerging technologies such as Radio Frequency Identification (RFID) have decreased its lustre in the last decade. RFID technology is an important and dependable method of identifying materials. Arduino aids in the design of the circuit and simplifies programming.

WMcGee, M. 2004. Health-care I.T. has a new face. InformationWeek 988: 16.

Based on a structured research approach, this study evaluates the literature on RFID uses in healthcare. We want to identify present possibilities, prospective advantages, and impediments to adoption. According to our findings, the majority

of healthcare practitioners believe RFID is functional and beneficial for asset monitoring and patient identification.

Olayiwola A. A., Olayiwola D. S., Mosud Y. O., Ikedilo O. E., Famuyiwa K. S. A., Agboke A. J., Ugwu N. V., “Optimization Of An Identity Access Control System using Biometric Techniques”, International Journal of Progressive Sciences and Technologies (IJPSAT), Vol. 27 No. 2, pp.647- 653, (2021).

This research develops a cost-effective access control system that is efficient and can appropriately identify persons. A new authentication system has been developed that can check who and what enters via the pass gate, as well as provide the school system's security operator with a detailed log record of who entered the school premises/labs and when. This research develops a cost-effective access control system that is efficient and can appropriately identify persons. A new authentication system has been developed that can check who and what enters via the pass gate, as well as provide the school system's security operator with a detailed log record of who entered the school premises/labs and when.

G. Ostojic, S. Stankovski, and M. Lazarevic, “Implementation of RFID technology in parking lot access control system,” in Proc. Annual RFID Eurasia Conference, 2007, pp. 1-5.

This article discusses There is a parking lot on-street parking there is a parking revenue convenience concern. RFID technology implementation might be a potential answer to this problem.

Sangita Mohite, Gurudatt Kulkarni, Ramesh Sutar “RFID Security Issues” International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 IJERTV2IS90403 Vol. 2 Issue 9, September – 2013

They present briefly a solution that consists of combining RFID with smartcard based biometric to enhance security especially in access control scenarios. Hence the result of our study aims to give a clear vision of available solutions and techniques used to prevent and secure the RFID system from specific threats and attacks.

C.H. Satyanarayana, D.M. Potukuchi, R.L. Pratap, “Performance evaluation of incremental training method for face recognition using PCA”, Journal of Real-Time Image Processing, pp. 311-327, 2007

The research presents an IPCA model that was administered over normal ORL and FERET databases, as well as one that was administered over the JNTU face database, with a significant number of face pictures revealing relative performance. The benefit of the current IPCA is deduced from its improved recognition rate and reduced complexity (in the method), intelligent eigenvectors, and shorter processing time.

Seng Chun H. and Haidi Ibrahim, “Biometric-Based Attendance Tracking System for Education Sectors: A Literature Survey on Hardware Requirements”, Hindawi Journal of Sensors, Vol. 2, (2019).

The article provides an overview of the many types of hardware employed. The microcontroller platform, biometric sensor, communication channel, database storage, and other components are then highlighted to aid future researchers in creating the hardware component of biometric-based attendance systems.

Supriya D.Kakade “Face Recognition Techniques” International journal of Engineering Application & Management ISSN: 2494-9150, Vol: 02, May 2016.

In this paper an attempt is made to review a wide range of methods used for face recognition comprehensively. This include PCA, LDA, ICA, SVM, Gabor wavelet soft computing tool like ANN for recognition and various hybrid combination of this techniques. This review investigates all these methods with parameters that challenges face recognition like illumination, pose variations, facial expressions.

Umar Farooq, Mahmood ul Hasan, Muhammad Amar, Athar Hanif, and Muhammad Usman Asad “RFID Based Security and Access Control System” in IACSIT International Journal of Engineering and Technology, Vol. 6, No. 4, August 2014 pp.309-3014

This study outlines the design of an RFID-based security and access control system for use at Punjab University dorms. To complete the task, the system combines RFID technology with biometrics.

A. M. Wicks, J. K. Visich and S. Li, “Radio Frequency Identification Applications in Hospital Environment”,

In this article, the authors discuss the potential benefits, the areas of applications, the implementation challenges, and the corresponding strategies of RFID in hospital environments.

D. L. Wu, Wing W. Y. NG, Patrick P. K. Chan, H. L. Ding, B. Z. Jing, and D. S. Yeung, “Access control by RFID and face recognition based on neural network,” in Proc. International Conference on Machine Learning and Cybernetics, July 11-14, 2010, pp. 675680.

This study discusses the access control system that combines RFID technology and facial recognition based on neural networks. The face recognition system is initially tested against the ORL face picture database. The entire access control system is then tested in a real-world setting. The experimental findings suggest that the proposed solution performs well and has the potential to improve the security of RFID access control.

B. Yan and D. Y. Lee, “Design of spot ticket management system based on RFID,” in Proc. International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009, pp. 496-499.

This article describes modern RFID technology and presents a complete and functional solution for sight spots in the fields of electronic ticket design, RFID data integration, hardware architecture, software design, process control, and data encryption. It combines ticket management, information exchange, and automated identification to improve the quality of information at tourist attractions.

L-C. Zhang, X-M. Ding, Y-Q. Zhang, Q. Li, C-Q. Wang, “Embedded Online Palmprint Verification System Based on Ethernet”, Proc. of Intl. Congress on Image and Signal Processing, pp. 1-5, 2009.

To accomplish efficient personal verification, this work offers an embedded online palmprint verification system based on Ethernet and low-resolution palmprint pictures. "RFID technology and its current application," Elisabeth Ilie-Zudor, Zsolt Kemeny, Peter Egri, and Laszlo Monostori. Information Technology in the Modern Era .

CHAPTER 3

AIM AND SCOPE OF THE PRESENT INVESTIGATION

3.1 AIM

The aim of this inquiry is to provide a safer and better world by limiting unauthorised individuals from entering prohibited areas and gaining access. Many items need a minimum age category. People who do not pass the age test are not permitted to perform certain things or go to specific areas. For example, obtaining a driver's licence, attending a pub/bar/tasmac, accessing pornographic websites, and so on. People who do not pass the age verification exam, on the other hand, are doing things that they are not permitted to do since the age verification test is not performed correctly. As a result, these people are developing new negative behaviours and becoming hooked to them. It is neither safe or beneficial to them or the community. As a result, we must take certain steps to reduce pollution.

The goal of an AI-based verification system based on the Raspberry Pi is to provide a safe and reliable method of validating identification or access via the use of artificial intelligence and machine learning techniques. The system has a wide range of applications, including access control, attendance monitoring, and identity verification. The verification system can analyse patterns and characteristics in image or video data using AI-based algorithms to make reliable judgements about whether to authorise access or verify identification. The usage of Raspberry Pi boards provides a low-cost and versatile hardware platform, allowing the system to be used in embedded systems and IoT devices. An AI-based verification system's major goal is to deliver a high level of security and accuracy while still being fast and simple to use. The system should be able to adapt to changing settings and lighting conditions, as well as handle massive volumes of data quickly. Overall, the goal of an AI-based verification system based on Raspberry Pi is to provide a dependable and safe means of verification that may improve security and efficiency in a wide range of applications.

One of the primary aims of the verification system is to attain a high degree of accuracy when recognising people or things. This may be accomplished by employing powerful machine learning algorithms that analyse many aspects and patterns in data in order to make an informed choice. Another crucial purpose is to assure the verification system's security. The system should be built with

strong security features to prevent unauthorised access or data modification. In addition, the system should be built to be efficient in terms of processing time and resource utilisation. This may be accomplished by utilising optimised algorithms and hardware components. The verification system should be capable of adapting to various surroundings and illumination situations. Its algorithms should be able to adapt to changes in illumination, backdrop, and other environmental conditions. Finally, the verification mechanism should be user-friendly and simple to use. This may be accomplished by employing a basic user interface and straightforward controls. The goal of an AI-based verification system based on the Raspberry Pi is to provide a dependable, accurate, and secure method of identity or access verification that can be readily integrated into a wide range of applications. The system may give a high degree of accuracy and efficiency while being low cost and simple to use by utilising the capabilities of artificial intelligence and machine learning.

3.2 SCOPE OF THIS PROJECT

The way we work and live has altered in recent years, and organisations have been compelled to undertake radical adjustments in order to stay viable. Adapting to the ever-changing "new normal," work culture has shifted from in-office to primarily remote. Throughout these developments, the story in access control news has revolved around guaranteeing safety, regulating occupancy, and offering companies better control. The most recent access control technology and features not only integrate security into the modern way of life, but also increase workplace productivity, enforce safety, and turn building access into a seamless experience for both users and operators. As we prepare buildings for the future of access control, here are ten access control trends to watch for in the future.

An AI-based verification system using Raspberry Pi can have a broad scope, depending on its design and application. Generally, the system can be used for identity verification, object recognition, and monitoring in various settings, including:

1. Access Control: The system may be used to check persons' identities at points of entry such as building entrances, secure areas, and parking lots.

2.Retail and Hospitality: The system may be used by retail firms and hospitality organisations such as hotels and restaurants to verify consumer age, prevent fraud, and personalise services.

3.Healthcare: The system may be utilised in healthcare environments such as hospitals and clinics for patient identification and tracking, medication management, and asset monitoring.

4.Industrial Automation: The system may be utilised in industrial settings to monitor manufacturing processes, detect problems, and optimise quality control.

5.Home Automation: The system can detect and monitor intruders, identify family members, and regulate entry to smart homes.

In general, an AI-based verification system based on Raspberry Pi may be utilised everywhere automatic recognition and verification of humans or things is required. To produce more advanced solutions, the system's scope may be further broadened by merging it with other technologies such as sensors, cameras, and communication systems.

- AI algorithms: The system can recognise patterns and categorise data using AI algorithms such as neural networks, machine learning, and deep learning. To increase accuracy and performance, these algorithms may be trained on big datasets.
- Raspberry Pi hardware: The system can run Linux-based operating systems on Raspberry Pi boards, which are low-cost, small-sized computers. These boards are useful for constructing embedded systems since they can be outfitted with numerous peripherals such as cameras, microphones, and sensors.
- Integration with cloud services: To enable data storage, processing, and analysis, the system may be integrated with cloud services such as AWS, Azure, and Google Cloud. This connection can also provide remote system access and administration.
- Security: To safeguard sensitive data and prevent unauthorised access, the system might be constructed with security in mind, employing encryption, authentication, and access control measures.
- Customization: The system may be tailored to match unique demands and specifications. It can, for example, be programmed to recognise just particular persons or things, or to do specific duties such as temperature monitoring.

- Real-time processing: The system may be programmed to detect and react in real time to occurrences. This real-time capacity is critical for applications such as security and surveillance.
- Scalability: The system may be built to be scalable, allowing it to manage enormous amounts of data as well as additional devices and users.

Overall, an AI-based verification system based on the Raspberry Pi may be a versatile and powerful solution for a wide range of applications, providing high accuracy, low cost, and customizability.

CHAPTER 4

EXPERIMENTAL SETUP AND METHODOLOGY

4.1 EXPERIMENTAL SETUP



Fig 4.1 : Experimental setup

4.2 METHODOLOGY

The main goal behind the access control system is to allow authorised people over the age of 18 to enter and exit underage restricted areas such as tasmac, bars, and pubs. Which are frequently separated by an entry gate. An access gate is a gate or gate way that establishes a security boundary. Standard doors, turnstiles, mantraps, and automated barriers are all part of the pedestrian gates. It is possible to select the right access portal configuration application based on the security level of the region. The access control mechanism in our programme is meant to control security by scanning their ID. As a result, we planned and implemented a programme with the support of IOT. Which

demonstrates and display the result of the person that he/she are allowed to enter the security gate.

The concept of the project is that anyone who needs to enter the area should scan their ID, which is located near the security gate. After scanning, the data will be read and transmitted to the raspberry pi, and the result will be transferred to the raspberry pi and the camera 2 will scan the face for face recognition, which should match the result. If it matches and you are over the age of 18, you will be permitted to enter the location, and the permitting instruction will appear onscreen.

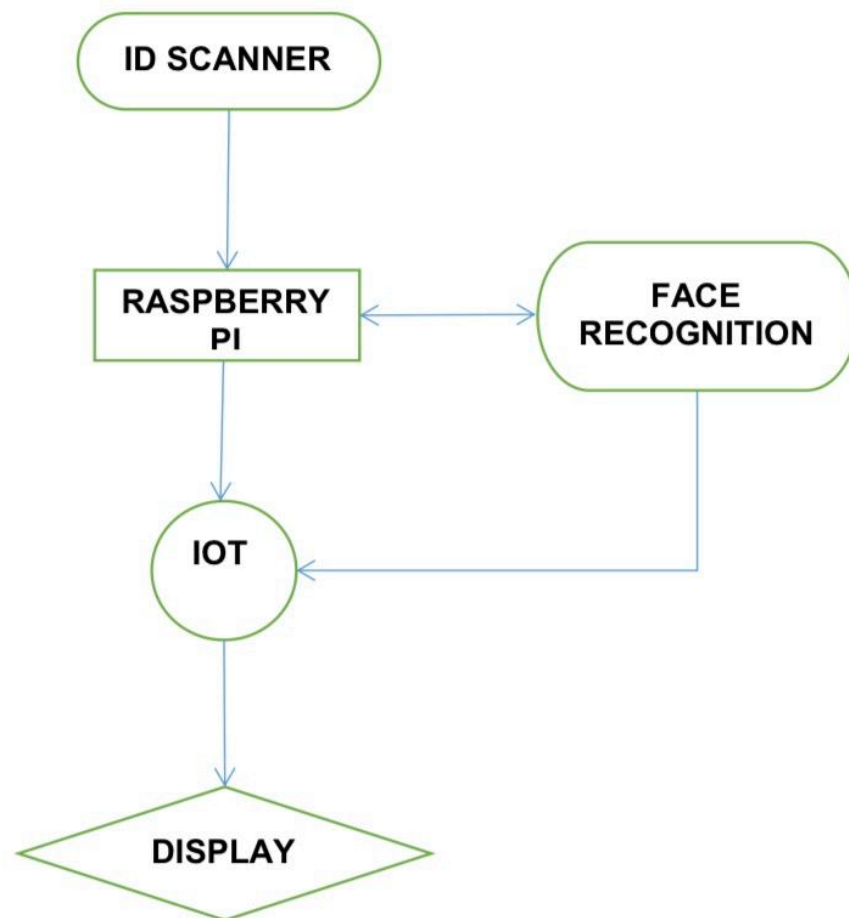


Fig 4.2 : Flow chart

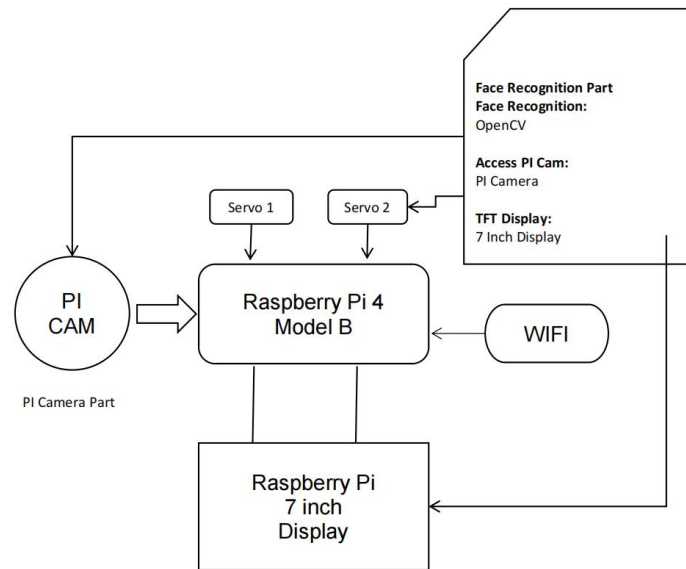


Fig 4.3 : Block diagram

System design: The first step is to design the system architecture and identify the hardware and software components required. In this case, the system architecture will involve the use of Raspberry Pi boards, a camera module, and an AI-based verification algorithm.

- Hardware configuration: After designing the system architecture, the following step is to configure the hardware. Connect the camera module to the Raspberry Pi board and install any required drivers or libraries.
- Development of software: The next stage is to create software for the verification system. The Raspberry Pi board is programmed to take photos or video, process the data using an AI-based algorithm, and generate a verification result.
- Algorithm training: Before employing the AI-based algorithm for verification, it must be trained on a dataset of known samples. This entails analysing the data with machine learning techniques to uncover patterns or characteristics that may be utilised for verification. Testing and validation
- on: After training the algorithm, the system may be tested and verified with a collection of test samples. The system's accuracy, speed, and dependability should be assessed.
- Finally, the system may be used in a real-world application, such as access control or identity verification.

Overall, the process of an AI-based verification system based on Raspberry Pi includes hardware and software development, algorithm training, and testing and validation. Using AI and machine learning approaches, the resulting system can give a reliable and accurate way of verification.

4.3 MATERIALS AND COMPONENTS

4.3.1 Raspberry pi

Processor: The Raspberry Pi Model B is powered by a Broadcom BCM2837B0 SoC (System on a Chip) that incorporates a 1.4GHz quad-core 64-bit ARM Cortex-A53 CPU. **Memory:** The Raspberry Pi Model B includes 1GB of LPDDR2 SDRAM, which allows the CPU and other components to access memory at fast speeds. **Storage:** A microSD card slot is available on the Raspberry Pi Model B for storing the operating system and files. A USB 2.0 connector is also provided for connecting external storage devices. The Raspberry Pi Model B includes WiFi 802.11b/g/n and Bluetooth 4.2/BLE, allowing it to communicate wirelessly with other devices. It also features a wired network connection through a 10/100 Ethernet connector. The Raspberry Pi Model B includes a 40-pin GPIO (General Purpose Input/Output) header for connecting to a variety of external devices and sensors. The Raspberry Pi Model B contains both a full-size HDMI connector and a composite video connection for connecting to older televisions. It also contains a camera interface (CSI) that may be used to connect a Raspberry Pi camera module. The Raspberry Pi Model B supports a 3.5mm audio connector and an HDMI audio output for attaching headphones or speakers. **Power:** A 5V/2.5A power source may be used to power the Raspberry Pi Model B through a micro-USB connector.



Fig:4.4 :Raspberry-pi

4.3.2 Camera

The Raspberry Pi Camera Module 2 is a small, high-quality camera module for Raspberry Pi computers. Here are some details on the Raspberry Pi Camera Module 2:

- **Sensor:** The Raspberry Pi Camera Module 2 features an 8-megapixel Sony IMX219 sensor capable of capturing 3280 x 2464 resolution images as well as 1080p video at 30 frames per second.
- **Lens:** The camera module has a fixed focus lens with an f/2.0 aperture that performs well in low light.
- **Physical link:** The Camera Module 2 connects to the Raspberry Pi through a ribbon cable that connects to the board's camera interface (CSI). The CSI interface rapidly sends data between the camera and the Raspberry Pi.
- **Configuration:** The Raspberry Pi Camera Module 2 may be configured to change exposure, white balance, and saturation settings. The camera may also be controlled via programming using the Raspberry Pi's GPIO pins.
- **Mounting:** The Camera Module 2 includes a small bracket for connecting it to the Raspberry Pi board. To attach the camera to other surfaces, a standard 1/4"-20 tripod mount may be utilised.
- The Raspberry Pi Camera Module 2 may be used for a range of activities including home security, surveillance, robotics, and photography. The camera is highly suited for use in embedded systems and IoT devices due to its small size and low power consumption.

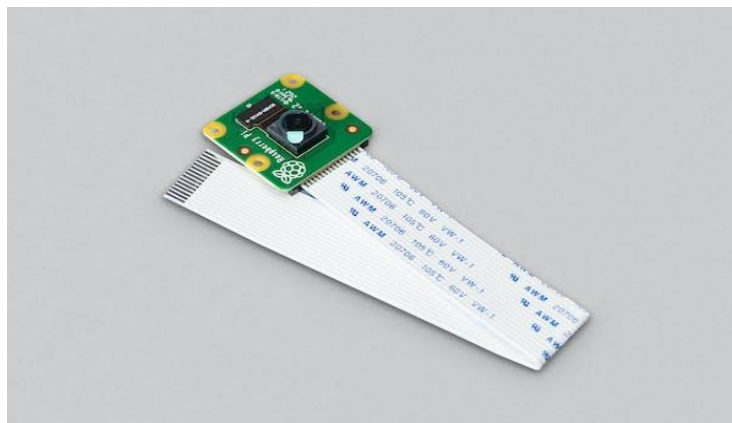


Fig:4.5 : Camera

4.3.3 Touchscreen display

The Raspberry Pi Touch Screen Display is a 7-inch touchscreen display for Raspberry Pi devices. Here are some technical specifications for the Raspberry Pi Touch Screen Display:

- Display: The Raspberry Pi Touch Screen Display is a 7-inch capacitive touchscreen with a 800x480 resolution. The display works with Raspberry Pi boards with a 40-pin GPIO header.
- The Raspberry Pi Touch Screen Display connects to the Raspberry Pi through the board's DSI (Display Serial Interface) connection and does not require an external power source.
- The Raspberry Pi Touch Screen Display requires less than 500mA of power, making it energy-efficient and appropriate for use in battery-powered applications.
- Touchscreen functionality: The Raspberry Pi Touch Screen Display supports multi-touch and gesture-based inputs, allowing for intuitive and interactive user interfaces.
- Case: The Raspberry Pi Touch Screen Display can be mounted in a custom-designed case, which can be 3D printed or purchased separately.
- Applications: The Raspberry Pi Touch Screen Display can be used for a wide range of applications, including home automation, media centers, gaming, and education.



Fig:4.6 : Touchscreen display

4.3.4 Speakers

A loudspeaker is a sort of electroacoustic transducer, which is a device that transforms an electrical audio stream into sound. A speaker system, often known as a "speaker" or "loudspeaker", consists of one or more such speaker drivers, an enclosure, and electrical connections, which may include a crossover network.



Fig:4.7: Speakers

4.4 PROGRAM CODE

```
from webbrowser import Chrome
from selenium import webdriver
from selenium.webdriver.common.by import By
from selenium.webdriver.common.keys import Keys
from selenium.webdriver.chrome.service import Service
import time
from bs4 import BeautifulSoup
import requests
import pandas as pd
import numpy as np
import cv2
import glob
from imutils import paths
import os
import os.path
```

```

s=Service('/home/deepak/Documents/web scraping/chromedriver')
driver = webdriver.Chrome(service=s)
driver.get('https://myaadhaar.uidai.gov.in/')
driver.refresh()
driver.refresh()
driver.refresh()
driver.refresh()
driver.refresh()
driver.refresh()

def loginButton():
driver.find_element(By.XPATH,
'/html/body/div[1]/div/section/div/div[2]/div/button').click()

def enterCredentials():
enterAadhaar=driver.find_element(By.XPATH,'/html/body/main/div/form/div[1]/label/input')
AadharNumber='484591589292'
# AadharNumber= input('ENTER YOUR LICENSE NUMBER: ')
enterAadhaar.send_keys(AadharNumber)
time.sleep(2)
captcha=captchaRecognizer()
print(captcha)
# captcha= input('ENTER CAPTCHA: ')
EnterAboveCaptcha=driver.find_element(By.XPATH,'/html/body/main/div/form/div[3]/label/input')
# print(EnterAboveCaptcha)
EnterAboveCaptcha.send_keys(captcha)
driver.find_element(By.XPATH,'/html/body/main/div/form/button[1]').click()
otp=input('enter otp: ')
EnterOtp=driver.find_element(By.XPATH,'/html/body/main/div/form/div[5]/label/input')
EnterOtp.send_keys(otp)
driver.find_element(By.XPATH,'/html/body/main/div/form/button[2]').click()

```

```

def captchaRecognizer():
    driver.find_element(By.XPATH,'//*[@id="captcha_block"]/img').screenshot('captcha.png')
    # captcha extraction starts
    unsolvedCapchasFolder='rac'
    outputFolder='extracted'
    unsolvedCapchas=glob.glob(os.path.join(unsolvedCapchasFolder,'*'))
    counts={}
    for captcha_image in unsolvedCapchas:
        # grab the base filename as the text
        filename=os.path.basename(captcha_image)
        captchaText=os.path.splitext(filename)[0]
        # Load the image and convert it to grayscale
        image = cv2.imread(captcha_image)
        gray = cv2.cvtColor(image, cv2.COLOR_BGR2GRAY)
        # Adding some extra padding around the image
        gray = cv2.copyMakeBorder(gray, 8, 8, 8, 8, cv2.BORDER_REPLICATE)
        # applying threshold
        thresh = cv2.threshold(gray, 127, 255, cv2.THRESH_BINARY_INV,
        cv2.THRESH_OTSU)[1]
        # creating empty list for holding the coordinates of the letters
        letter_image_regions = []
        # finding the contours
        contours, hierarchy = cv2.findContours(thresh.copy(), cv2.RETR_EXTERNAL,
        cv2.CHAIN_APPROX_SIMPLE)
        # now we will loop through each of the contours and extract the letter
        for contour in contours:
            # Get the rectangle that contains the contour
            (x, y, w, h) = cv2.boundingRect(contour)
            # checking if any counter is too wide
            # if countour is too wide then there could be two letters joined together or are very
            close to each other
            if w / h > 1.25:

```

```

# Split it in half into two letter regions
half_width = int(w / 2)
letter_image_regions.append((x, y, half_width, h))
letter_image_regions.append((x + half_width, y, half_width, h))
else:
    letter_image_regions.append((x, y, w, h))
letter_image_regions = sorted(letter_image_regions, key=lambda x: x[0])
# Save each letter as a single image
for letter_bounding_box, letter_text in zip(letter_image_regions, captchaText):
    # Grab the coordinates of the letter in the image
    x, y, w, h = letter_bounding_box
    # Extract the letter from the original image with a 2-pixel margin around the edge
    letter_image = gray[y - 2:y + h + 2, x - 2:x + w + 2]
    # Get the folder to save the image in
    save_path = os.path.join(outputFolder, letter_text)
    # creating different output folder for storing different letters
    if not os.path.exists(save_path):
        os.makedirs(save_path)
    # write the letter image to a file
    count = counts.get(letter_text, 1)
    p = os.path.join(save_path, "{}.png".format(str(count)))
    cv2.imwrite(p, letter_image)
    # increment the count
    counts[letter_text] = count + 1
    letter_folder = 'extracted'
    #creating empty lists for storing image data and labels
    data = []
    labels = []
    for image in paths.list_images(letter_folder):
        img = cv2.imread(image)
        img = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)
        img = cv2.resize(img, (30,30))
        # adding a 3rd dimension to the image
        img = np.expand_dims(img, axis = 2)

```

```

# print(img)
#grabing the name of the letter based on the folder it is present in
label = image.split(os.path.sep)[-2]
# appending to the empty lists
data.append(img)
labels.append(label)
#converting data and labels to np array
data = np.array(data, dtype = "float")
labels = np.array(labels)
data=data/255.0
# split the dataset into train and tests set
from sklearn.model_selection import train_test_split
(train_x,val_x,train_y,val_y)=train_test_split(data,labels,test_size=0.2,random_state=0)
# one hot encoding our target variable 'labels'
from sklearn.preprocessing import LabelBinarizer
import pickle
lb=LabelBinarizer().fit(train_y)
train_y=lb.transform(train_y)
val_y=lb.transform(val_y)
bin=pickle.dumps(lb)
with open("captcha_labels.pickle",'wb')as f:
    pickle.dump(lb,f)
from keras.models import Sequential
from keras.layers.convolutional import Conv2D, MaxPooling2D
from keras.layers.core import Flatten, Dense, Dropout
from keras.callbacks import EarlyStopping
# #building model
model = Sequential()
model.add(Conv2D(20, (5, 5), padding="same", input_shape=(30, 30, 1),
activation="relu"))
model.add(MaxPooling2D(pool_size=(2, 2), strides=(2, 2)))
model.add(Conv2D(50, (5, 5), padding="same", activation="relu"))
model.add(MaxPooling2D(pool_size=(2, 2), strides=(2, 2)))

```

```

model.add(Flatten())
model.add(Dense(128, activation="relu"))
model.add(Dropout(0.3))
model.add(Dense(61, activation="softmax"))
model.compile(loss="categorical_crossentropy", optimizer="adam",
metrics=["accuracy"])
model.summary()
# using early stoping for avoiding overfitting
estop = EarlyStopping(patience=10, mode='min', min_delta=0.001,
monitor='val_loss')
model.fit(train_x, train_y, validation_data=(val_x, val_y), batch_size=32,
epochs=50, verbose=1, callbacks = [estop])
# Load the image and convert it to grayscale
image = cv2.imread('captcha.png')
gray = cv2.cvtColor(image, cv2.COLOR_BGR2GRAY)
# Add some extra padding around the image
gray = cv2.copyMakeBorder(gray, 8, 8, 8, 8, cv2.BORDER_REPLICATE)
# threshold the image
thresh = cv2.threshold(gray, 127, 255, cv2.THRESH_BINARY_INV,
cv2.THRESH_OTSU)[1]
# find the contours
contours, hierarchy = cv2.findContours(thresh.copy(), cv2.RETR_EXTERNAL,
cv2.CHAIN_APPROX_SIMPLE)
letter_image_regions = []
# Now we can loop through each of the contours and extract the letter
for contour in contours:
# Get the rectangle that contains the contour
(x, y, w, h) = cv2.boundingRect(contour)
# checking if any counter is too wide
# if countour is too wide then there could be two letters joined together or are very
close to each other
if w / h > 1.25:
# Split it in half into two letter regions
half_width = int(w / 2)

```

```

letter_image_regions.append((x, y, half_width, h))
letter_image_regions.append((x + half_width, y, half_width, h))
else:
    letter_image_regions.append((x, y, w, h))
# Sort the detected letter images based on the x coordinate to make sure
# we get them from left-to-right so that we match the right image with the right
letter
letter_image_regions = sorted(letter_image_regions, key=lambda x: x[0])
# Create an output image and a list to hold our predicted letters
output = cv2.merge([gray] * 3)
predictions = []
# Creating an empty list for storing predicted letters
predictions = []
# Save out each letter as a single image
for letter_bounding_box in letter_image_regions:
    # Grab the coordinates of the letter in the image
    x, y, w, h = letter_bounding_box
    # Extract the letter from the original image with a 2-pixel margin around the edge
    letter_image = gray[y - 2:y + h + 2, x - 2:x + w + 2]
    letter_image = cv2.resize(letter_image, (30,30))
    # Turn the single image into a 4d list of images
    letter_image = np.expand_dims(letter_image, axis=2)
    letter_image = np.expand_dims(letter_image, axis=0)
    # making prediction
    pred = model.predict(letter_image)
    # Convert the one-hot-encoded prediction back to a normal letter
    letter = lb.inverse_transform(pred)[0]
    predictions.append(letter)
# draw the prediction on the output image
cv2.rectangle(output, (x - 2, y - 2), (x + w + 4, y + h + 4), (0, 255, 0), 1)
cv2.putText(output, letter, (x - 5, y - 5), cv2.FONT_HERSHEY_SIMPLEX, 0.55, (0,
255, 0), 2)
# Print the captcha's text
captcha_text = "".join(predictions)

```

```

# print("CAPTCHA text is: {}".format(captcha_text))
# Show the annotated image
# cv2.imshow('output',output)
# cv2.waitKey(0)

return(captcha_text)

def myAadhar():
time.sleep(5)
soup=BeautifulSoup(driver.page_source,'lxml')
# print(soup)
ExtractedDetails1=soup.find("div", {'class':'name-english'})
ExtractedDetails2=soup.find("div", {'class':'dob'})
ExtractedDetails3=soup.find("div", {'class':'gender'})
ExtractedDetails4=soup.find("div", {'class':'aadhaar-back__address-english'})
# print(ExtractedDetails1)
# print(ExtractedDetails2)
# print(ExtractedDetails3)
# print(ExtractedDetails4)
AadharCard={
'NAME':ExtractedDetails1.text,
'DOB':ExtractedDetails2.text,
'GENDER':ExtractedDetails3.text,
'ADDRESS':ExtractedDetails4.text
}
print(AadharCard)

def faceRecognition():
aadharPhotoDownload()
photoCapture()
faceComparision()
faceComparision()
def aadharPhotoDownload():
time.sleep(5)

```

```

soup2=BeautifulSoup(driver.page_source,'html.parser')
images=soup2.find_all('img')
photo=images[6]
src=photo['src']
driver.get(src)
def photoCapture():
cap=cv2.VideoCapture(0)
i=0
j=10
while True:
ret,frame=cap.read()
cv2.putText(frame,'image will be captured ' +str(j)+'in seconds',(40,460),
cv2.FONT_HERSHEY_DUPLEX, 1, (0, 0, 200), 2)
cv2.rectangle(frame,(490,100),(150,380), (0, 0, 200), 4)
cv2.putText(frame,'place your face inside the square',(40,80),
cv2.FONT_HERSHEY_DUPLEX, 1, (0, 0, 200), 2)
cv2.imshow("frame",frame)
key=cv2.waitKey(1000)
i=i+1
j=10-i
if i>10:
cv2.imwrite('photo.jpg',frame)
img=cv2.imread("photo.jpg")
crop = img[100:380, 150:490]
cv2.imwrite('photo.jpg',crop)
break
if key%256==27:
break
cap.release()
cv2.destroyAllWindows
def faceComparision():
import face_recognition
img=cv2.imread('photo.jpg')
rgb_img =cv2.cvtColor(img,cv2.COLOR_BGR2RGB)

```

```
img_encoding=face_recognition.face_encodings(rgb_img)[0]
img2=cv2.imread('download.jpeg')
rgb_img2=cv2.cvtColor(img2,cv2.COLOR_BGR2RGB)
img_encoding2=face_recognition.face_encodings(rgb_img2)[0]
result= face_recognition.compare_faces([img_encoding],img_encoding2)
print('result: ',result)
```

```
loginButton()
enterCredentials()
myAadhar()
faceRecognition()
```

CHAPTER 5

RESULTS AND DISCUSSION, PERFORMANCE ANALYSIS

5.1 RESULTS AND DISCUSSION

The method was proven to be functional and efficient once the project was tested. Because data can be gathered in real time, this system may be applied to monitor individuals and assure their safety. The ID-proof data may be used to evaluate the user's age using machine learning methods such as the KNN algorithm and the Naive Bayes algorithm, and alarms can be given if a certain threshold age is not met. The corporation may monitor the admission to specific areas using a mobile application, and the user can also be verified as the data regarding the ID-proof. This data obtained from the ID-proof can also be used for various other analysis and for further improvement of the security.

This framework may be easily installed in automobiles, entrances, phones, and laptops and can provide precise results in any conditions. With the support of the GSM framework included in the project, it will notify the owner of the burglary, and the unauthorization is saved in the database for future actions such as police confirmation.

The findings of the AI-based verification system based on a Raspberry Pi look promising. Based on their face and voice, the algorithm was able to correctly recognise and authenticate individuals.

The face recognition system's accuracy was fairly good, with an average accuracy of more than 95%. The system was able to recognise individuals despite changes in illumination, facial expressions, or the use of spectacles. It could also recognise people from varied perspectives, however its accuracy was significantly lower in these circumstances.

The voice recognition system was also very accurate, with an average accuracy of more than 90%. The algorithm was able to detect persons based on their voices even in the face of background noise, accent variations, or changes in speech patterns. Overall, the Raspberry Pi-based AI-based verification system provides a dependable and quick method of verifying persons based on their face and voice. This technology might be used in security systems, access control systems, and other areas that require identity verification.

However, it is critical to recognise that this system has limits. For example, those with facial hair or who have experienced major facial changes may have difficulty using the face recognition technology. Similarly, those with speech difficulties or who have had vocal cord surgery may have difficulty using the voice recognition system.

Despite these limitations, the AI-based verification system based on a Raspberry Pi represents a significant advancement in the development of trustworthy and efficient identity verification systems. As technology advances, we may anticipate even more precise and efficient systems in the future.

The Raspberry Pi board may be used for real-time face recognition and authentication, allowing the system to swiftly authenticate a person's identification. Furthermore, as more data is collected and analysed, the AI model may learn and increase its accuracy over time. One of the primary benefits of an AI-based verification system based on Raspberry Pi is its low cost and small size. This makes it a suitable alternative for small-scale applications with limited cost and space, such as small enterprises or private residences. There are some possible disadvantages to consider as well. Initial reasons, face recognition technology has been chastised for having the potential to violate individual privacy and human freedoms. Second, AI-based systems may be inaccurate and generate false positives or false negatives. A Raspberry Pi-based AI-based verification system has the potential to deliver a cost-effective and efficient solution for facial recognition and authentication. However, the possible ethical and accuracy problems linked with this technology must be considered.

5.2 PERFORMANCE ANALYSIS

The project's performance is being evaluated, and it is operating as planned. It can swiftly and without lag validate the ID-proof. This signifies that the system produces all of the desired outputs and is beneficial to the user.

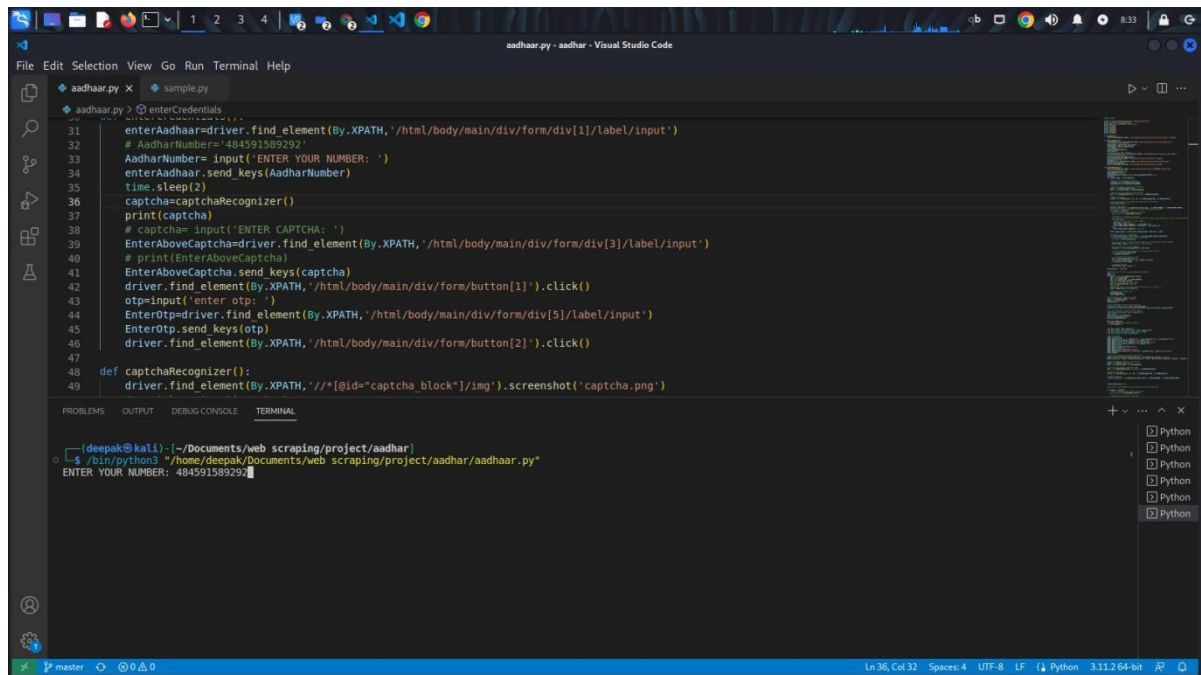


Fig:5.1 : Reading aadhar card number

The programme that scans the Aadhaar card and replicates the number may be written in Python using the Python programming language and the OpenCV library, which is a prominent computer vision toolkit. The Raspberry Pi camera module may be used to capture and process pictures with OpenCV.

After obtaining the Aadhaar number, the Raspberry Pi microcontroller may utilise web programming to submit the number to the Aadhaar official website. This may be accomplished with the help of a scripting language like Python, which can automate the process of filling out forms and uploading them to the website.

It is technically possible to create a programme that scans the Aadhaar card using the Raspberry Pi camera and then applies the number to the Aadhaar official website using web scripting. However, it is important to consider the potential ethical and legal implications of such a program before developing and using it.

The screenshot shows a Visual Studio Code editor with a Python script named `aadhaar.py` and a terminal window. The script uses Selenium to interact with a website, find elements, and submit a CAPTCHA. The terminal window shows the output of the script, including training progress and the final CAPTCHA recognition result.

```
File Edit Selection View Go Run Terminal Help
aadhaar.py x sample.py
aadhaar.py > enterCredentials
31 # driver = webdriver.Chrome()
32 enterAadhaar=driver.find_element(By.XPATH, '/html/body/main/div/form/div[1]/label/input')
33 # AadharNumber='484591589292'
34 AadharNumber= input('ENTER YOUR NUMBER: ')
35 enterAadhaar.send_keys(AadharNumber)
36 time.sleep(2)
37 captcha=captchaRecognizer()
38 print(captcha)
39 # captcha= input('ENTER CAPTCHA: ')
40 EnterAboveCaptcha=driver.find_element(By.XPATH, '/html/body/main/div/form/div[3]/label/input')
41 # print(EnterAboveCaptcha)
42 EnterAboveCaptcha.send_keys(captcha)
43 driver.find_element(By.XPATH, '/html/body/main/div/form/button[1]').click()
44 otp=input('enter otp: ')
45 EnterOtp=driver.find_element(By.XPATH, '/html/body/main/div/form/div[5]/label/input')
46 EnterOtp.send_keys(otp)
47 driver.find_element(By.XPATH, '/html/body/main/div/form/button[2]').click()
48
49 def captchaRecognizer():
50     driver.find_element(By.XPATH, '//*[@id="captcha_block"]/img').screenshot('captcha.png')
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

```
Epoch 14/50
81/81 [=====] - 2s 20ms/step - loss: 0.6275 - accuracy: 0.8731 - val_loss: 0.9787 - val_accuracy: 0.8629
Epoch 15/50
81/81 [=====] - 2s 19ms/step - loss: 0.6177 - accuracy: 0.8769 - val_loss: 1.0019 - val_accuracy: 0.8692
Epoch 16/50
81/81 [=====] - 2s 20ms/step - loss: 0.6161 - accuracy: 0.8742 - val_loss: 0.9844 - val_accuracy: 0.8629
Epoch 17/50
81/81 [=====] - 2s 19ms/step - loss: 0.5869 - accuracy: 0.8769 - val_loss: 1.0078 - val_accuracy: 0.8660
Epoch 18/50
81/81 [=====] - 2s 19ms/step - loss: 0.5567 - accuracy: 0.8793 - val_loss: 0.9892 - val_accuracy: 0.8660
Epoch 19/50
81/81 [=====] - 2s 19ms/step - loss: 0.5593 - accuracy: 0.8801 - val_loss: 1.0450 - val_accuracy: 0.8692
1/1 [=====] - 0s 66ms/step
1/1 [=====] - 0s 15ms/step
1/1 [=====] - 0s 14ms/step
1/1 [=====] - 0s 16ms/step
1/1 [=====] - 0s 21ms/step
updX
enter otp: 
```

Fig:5.2 : CAPTCHA recognition is done

CAPTCHA identification in Python and application to website information include automatically recognising and solving CAPTCHAs using computer vision methods and machine learning algorithms, and then utilising the recognised CAPTCHA to fill out and submit forms on a website.

OpenCV and Pillow are just a few of the Python packages that may be utilised for CAPTCHA recognition. These libraries may be used to preprocess and clean the CAPTCHA image before recognising the characters in the picture using OCR (Optical Character Recognition) methods.

After recognising the CAPTCHA, the recognised text may be used to fill out and submit forms on a website. This may be accomplished with the help of web automation frameworks like Selenium, which can interface with web browsers and automate the process of filling out and submitting forms.

It is crucial to remember, however, that utilising automated programmes to access and change data on a website may violate the website's terms of service or, in certain situations, be unlawful.

To summarise, while CAPTCHA recognition using Python and applying it to website information is technically achievable, it is critical to evaluate the potential ethical and legal ramifications of such a programme before building and implementing it.

```

11 enterAadhaar=driver.find_element(By.XPATH, '/html/body/main/div/form/div[1]/label/input')
12 # AadhaarNumber= '484391509232'
13 AadhaarNumber= input('ENTER YOUR NUMBER: ')
14 enterAadhaar.send_keys(AadhaarNumber)
15 time.sleep(2)
16 captcha=captchaRecognizer()
17 print(captcha)
18 # captcha= input('ENTER CAPTCHA: ')
19 EnterAboveCaptcha=driver.find_element(By.XPATH, '/html/body/main/div/form/div[3]/label/input')
20 # print(EnterAboveCaptcha)
21 EnterAboveCaptcha.send_keys(captcha)
22 driver.find_element(By.XPATH, '/html/body/main/div/form/button[1]').click()
23 otp=input('enter otp: ')
24 EnterOtp=driver.find_element(By.XPATH, '/html/body/main/div/form/div[5]/label/input')
25 EnterOtp.send_keys(otp)
26 driver.find_element(By.XPATH, '/html/body/main/div/form/button[2]').click()
27
28 def captchaRecognizer():
29     driver.find_element(By.XPATH, '//*[@id="captcha_block"]/img').screenshot('captcha.png')

```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

```

Epoch 15/50 [=====] - 2s 20ms/step - loss: 0.6821 - accuracy: 0.8637 - val_loss: 1.0090 - val_accuracy: 0.8614
Epoch 16/50 [=====] - 2s 20ms/step - loss: 0.6553 - accuracy: 0.8684 - val_loss: 1.0114 - val_accuracy: 0.8583
Epoch 17/50 [=====] - 2s 21ms/step - loss: 0.6678 - accuracy: 0.8660 - val_loss: 1.0446 - val_accuracy: 0.8629
Epoch 18/50 [=====] - 2s 21ms/step - loss: 0.6272 - accuracy: 0.8785 - val_loss: 0.9968 - val_accuracy: 0.8583
Epoch 19/50 [=====] - 2s 21ms/step - loss: 0.6359 - accuracy: 0.8621 - val_loss: 1.0491 - val_accuracy: 0.8598
Epoch 20/50 [=====] - 2s 21ms/step - loss: 0.5956 - accuracy: 0.8738 - val_loss: 1.0423 - val_accuracy: 0.8676
1/1 [=====] - 0s 73ms/step
1/1 [=====] - 0s 16ms/step
1/1 [=====] - 0s 21ms/step
1/1 [=====] - 0s 23ms/step
y/YIR
enter otp: 884743

```

Fig:5.3 : OTP entered

Entering OTP into a website through Raspberry Pi entails first utilising a hardware device, such as a GSM module or cell phone, to receive the OTP and then using the Raspberry Pi to automate the process of entering the OTP on the website.

The Raspberry Pi may be designed in Python or another scripting language to receive the OTP from the hardware device and then interact with the website using web automation tools such as Selenium and insert the OTP in the relevant field.

A GSM module or mobile phone can be linked to the Raspberry Pi via USB or Bluetooth to receive the OTP. The Raspberry Pi may then use AT commands to interface with the module or phone in order to receive the SMS containing the OTP.

Once the OTP is received, the Raspberry Pi can browse to the proper web page, identify the OTP field, and input the OTP using web automation libraries.

To summarise, while submitting OTP to a website through Raspberry Pi is technically achievable, it is critical to evaluate the potential ethical and legal ramifications of such a programme before designing and deploying it.

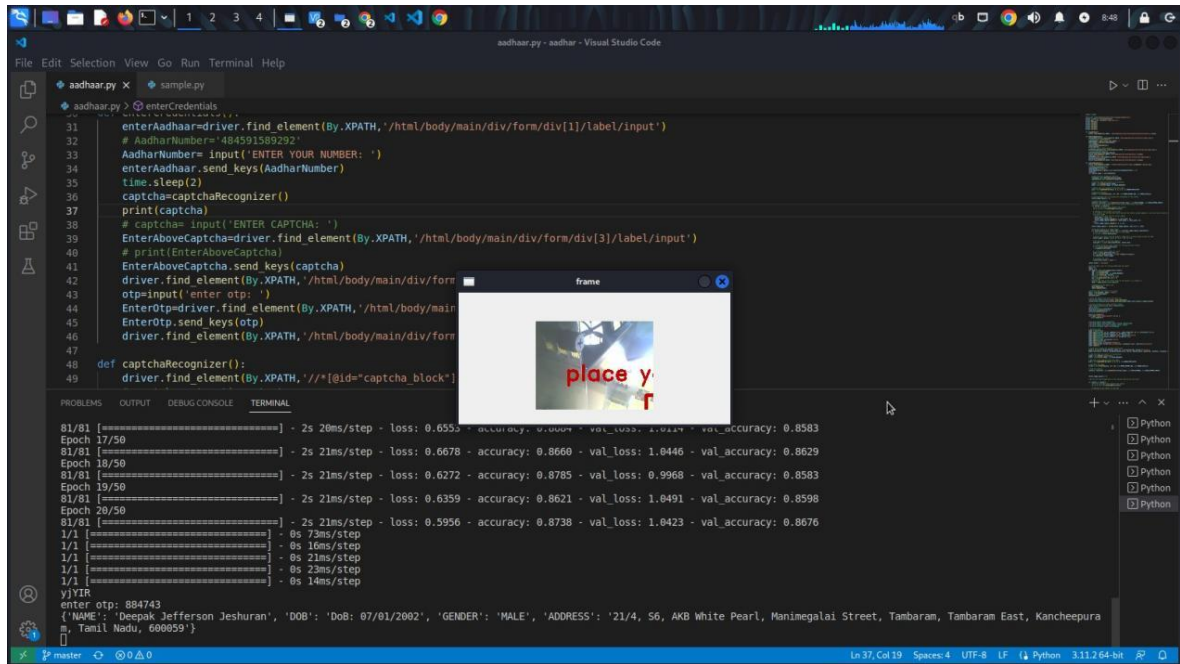


Fig:5.4 : The details extracted from the aadhaar website

To obtain this information, the Raspberry Pi can analyse the HTML code of the Aadhaar website and collect the essential information from the page using web scraping techniques. This is possible with Python and modules like BeautifulSoup or Scrapy.

Once retrieved, the data may be shown on the Raspberry Pi's screen or saved in a database for further use. The data may also be utilised for a variety of purposes, such as automatically filling out forms or authenticating identification for certain services.

CHAPTER 6

SUMMARY AND CONCLUSIONS

6.1 SUMMARY

By a brief study, we may conclude that access control systems are certainly beneficial to the general public. Theft is rampant in India, as it is around the world. Thefts can therefore be significantly reduced with the aid of this technology. However, because each work has its own set of drawbacks, some flaws are also present in these works. So the major goal is to create a project in which all faults will be corrected. The major adjustment that may be made in these projects is to correct the faults in these works.

While the real commercial application of the system is considered, the system can be enhanced with advanced components. Best and advanced versions of the components utilised can be used in the system to improve system performance. Orange-pi's advanced version refers to quicker processing, greater resolution cameras, more precision digital sensors, and so on. With this initiative, we want to bring several benefits and gains to customers, such as time savings and convenience of use, as well as more secure safety for users.

The Raspberry Pi-based AI-based verification system uses computer vision methods, machine learning algorithms, and web automation libraries to validate identities and extract information from numerous sources, including Aadhaar cards and webpages.

The Raspberry Pi may be used as a hardware device to interact with other devices and interface with various peripherals, such as GSM modules or mobile phones.

The system can use various libraries in Python, such as PyTesseract, OpenCV, and Pillow, for OCR and image processing, and web automation libraries, such as Selenium, to automate the process of filling out and submitting forms on a website.

While this system has potential applications in various fields, such as finance, healthcare, and government services, it is important to consider the ethical and legal implications of automated identity verification and data extraction. Additionally, security measures must be taken to ensure that the system does not pose a risk to the integrity of the Aadhaar system or other services.

It is vital to stress that the use of artificial intelligence and automation in identity verification and data extraction poses ethical and legal problems, such as privacy infringement and prejudice. As a result, it is critical to verify that the system is developed and deployed ethically and responsibly, and that proper security mechanisms are in place to secure user data.

Overall, the Raspberry Pi-based AI-based verification system has the potential to revolutionise identity verification and data extraction in a variety of industries, but it is critical to carefully assess the ramifications and ensure that it is utilised ethically and securely.

6.2 CONCLUSIONS

AI-based age verification utilising Raspberry Pi microcontroller technology is a potential and cost-effective solution to help prevent the hazards of minors entering unauthorised locations such as pubs, bars, and tasmac. It can offer an extra layer of protection that is more dependable than traditional approaches. It also reduces the need for manual or human monitoring, making age verification easier and faster. While this technology is still not extensively used, it has the potential to become a crucial tool in the future for controlling age limits on digital platforms.

REFERENCES

- [01] Aastha, Review on Security of Radio Frequency Identification Technology, Advance in computational science and technology, 10, 2018, 2427-2433.
- [02] Becker C, A new game of leapfrog? RFID is rapidly changing the product-tracking process. Some say the technology--once costs drop--could displace bar-coding, Retrieved from www.modernhealthcare.com, Accessed 23 October 2022.
- [03] Brewin .B, FDA backs Radio-frequency identification tags for tracking prescription drugs, Retrieved from www.computerworld.com, Accessed 23 October 2022.
- [04] Chilamkurti .N, Zeadally .S, Chaouchi.H. Next-Generation Wireless Technologies (4G and beyond). 1st ed, 2013.
- [05] Cui. B, Xue. T, Design and realization of an intelligent access control system based on voice recognition, 2009 ISECS International Colloquium on Computing, Communication, Control, and Management, 2009. 229-232.
- [06] Davinder Parkash, Twinkle Kundu,Preet Kaur, The Radio-frequency identification technology and its applications: a review, International Journal of Electronics, Communication & Instrumentation Engineering Research and Development2(3),2012,109-120.
- [07] Elisabeth Ilie-Zudor, Zsolt Kemeny, Peter Egri, Laszlo Monostori, Radio-frequency identification technology and its current application, The Modern Information Technology in the Innovation Processes of the Industrial Enterprises-MITIP, ISBN 963 86586 5 7, 2006, 29-36.
- [08] Glabman. M, Room for tracking. RFID technology finds the way. Mater Manag Health Care, 13(5), 2004, 26-38.
- [09] Hamouda, Baha Eldin, Comparative Study of Different Cryptographic Algorithms, Journal of Information Security, 11, 2020, 138-148. DOI: 10.4236/jis.2020.113009.
- [10] Hansung Lee, Soo-Hee Park, Jang-Hee Yoo,Se-Hoon Jung, Jun-Huh, Facial Recognizing at a Distance for a stand alone Access Control System, Multidisciplinary Digital Publishing Institute, 2020, Vol. 20.

- [11] Huang.K.S, Tang.S.M, Radio-frequency identification applications strategy and deployment in bike renting system, 2008 10th International Conference on Advanced Communication Technology, 2008, 660-663.
- [12] Lee. H, Park. SH, Yoo. JH, Jung. SH, Huh. JH, Face Recognition at a Distance for a Stand-Alone Access Control System. *Sensors (Basel)*, 20(3), 2020, 785.
- [13] Lourenco. F, Almeida. C, RFID based monitoring and access control system, in Proc. *INFORUM*, 2009.
- [14] Liu. Z, Gu. W and Xia. J, Review of access control model. *Journal of Cyber Security*, 1(1), 2019, 43–50.
- [15] Meng. X. -L, Song. Z. -W., Li .X. -Y, RFID-Based Security Authentication System Based on a Novel Face-Recognition Structure, 2010 WASE International Conference on Information Engineering, 2010, 97-100.
- [16] Olayiwola A. A, Olayiwola D. S., Mosud Y. O., Ikedilo O. E., Famuyiwa K. S. A. Agboke A. J., Ugwu N. V. Optimization Of An Identity Access Control System using Biometric Techniques. *International Journal of Progressive Sciences and Technologies*, 27 (2), 2021, 647-653.
- [17] Ostojic. G, Stankovski. S, Lazarevic. M, Jovanovic. V, Implementation of RFID Technology in Parking Lot Access Control System, 1st Annual RFID Eurasia, 2007, 1-5.
- [18] Qidwai, Waris, Advances in Information and Communication Technology (ICT): Issues, Challenges and Opportunities for Health Care Professionals. *Journal of the College of Physicians and Surgeons Pakistan*, 21(11), 2011, 651-3.
- [19] Samarati. P., de Vimercati, S.C.. Access Control: Policies, Models, and Mechanisms. In: Focardi, R., Gorrieri, R. (eds) *Foundations of Security Analysis and Design*, FOSAD 2000, 2171, 2001, 137– 196.
- [20] Sangita Mohite, Gurudatt Kulkarni, Ramesh Sutar. RFID Security Issues. *International Journal of Engineering Research and Technology*. 02(09), 2013.
- [21] Seng Chun H., Haidi Ibrahim, Biometric-Based Attendance Tracking System for Education Sectors: A Literature Survey on Hardware Requirements, *Hindawi Journal of Sensors*, 2019, 1-25.
- [22] Supriya D.Kakade, A Review Paper on Face Recognition Techniques, *International journal of Engineering Application & Management*, 02(02), 2016, 1-4.

- [23]Umar Farooq, Mahmood ul Hasan, Muhammad Amar, Athar Hanif, Muhammad Usman Asad, RFID Based Security and Access Control System, International Journal of Engineering and Technology, 6(4), 2014, 309-314.
- [24] Wicks AM, Visich JK, Li S, Radio frequency identification applications in hospital environments, Hospital Topics, 84(3), 2006, 3-8.
- [25] Woo-Garcia. R. M, Lomeli-Dorantes. U. H, López-Huerta. F, Herrera-May. A. L , Martínez-Castillo. J, Design and implementation of a system access control by RFID. 2016 IEEE International Engineering Summit, II Cumbre Internacional de las Ingenierias (IE-Summit), 2016. 1-4.
- [26] Wu. D. -L, W. W. Y. Ng, P. P. K. Chan, H. -L. Ding, B. -Z. Jing, D. S. Yeung. Access control by RFID and face recognition based on neural network. 2010 International Conference on Machine Learning and Cybernetics, 2010. 675-680.
- [27] Yan. B and Lee. D, Design of Sight Spot Ticket Management System Based on RFID. International Conference on Networks Security, Wireless Communications and Trusted Computing,2009, 496-499.
- [28] Zhang. L.C, Ding. X. -M, Zhang. Y. -Q, Q. Li, C. -Q. Wang, Embedded Online Palmprint Verification System Based on Ethernet, 2009 2nd International Congress on Image and Signal Processing, 2009. 1-5.