iHACS: Intelligent Home Access Control System

Capstone Project Report

Final Panel Evaluation

Submitted by:

401503008 - Brahmrita Singh

401503009 - Chinmaya Garg

401503015 - Kushagra Sharma

401553002 - Jashan Singh Sadioura

BE Fourth Year, COE

CPG No: 46

Under the Mentorship of

Prof. R.K. Sharma

Computer Science and Engineering Department

TIET, Patiala

November 2018

`

ABSTRACT

Internet of Things(IoT) has seen a steady growth over recent years – smart home appliances, smart personal gear, personal assistants and many more. The same is true for the field of biometrics where the need for automatic and secure recognition schemes have spurred the development of fingerprint and face recognition mechanisms found today in most smart phones and similar hand-held devices. Devices used in the Internet of Things (IoT) are often low-powered with limited computational resources. This means that biometric recognition pipelines aimed at IoT need to be streamlined and to be made as efficient as possible. Towards this end, we describe in this project how image-based biometrics can be leveraged in an IoT environment using a Raspberry Pi. We present a proof-of-concept image based system, secured by a face-recognition procedure, that gives authorized users access to their home space .

Our goal is to explore the operation ability of implementing Raspberry Pi based face recognition system using face detection and recognition techniques such as Haar detection and PCA. This project aims at taking face recognition to a level in which the system can replace the locking system of high security systems and buildings. With the use of the Raspberry Pi kit, we aim at making the system cost effective and easy to use, with better performance.

DECLARATION

We hereby announce that the design principles and working model of the project entitled iHACS: Intelligent Home Access Control System is an authentic record of our efforts carried out in the Computer Science and Engineering Department, TIET, Patiala, under the guidance of Dr. R. K. Sharma during 7th semester of our B.E. (Computer Engineering)

Date:18/11/2018

Registration No.	Name	Signature
401503008	Brahmrita Singh	
401503009	Chinmaya Garg	
401503015	Kushagra Sharma	
401553002	Jashan Sadioura	

Counter Signed By:

Faculty Mentor:

R.K. Sharma

Computer Science & Engineering Department,

TIET, Patiala

ACKNOWLEDGEMENT

We would like to express our thanks to our mentor Prof. R.K. Sharma. He has been of great help in our venture, and an indispensable resource of technical knowledge. He is truly an amazing mentor to have.

We are also thankful to Dr. Maninder Singh, Head, Computer Science and Engineering Department, entire faculty and staff of Computer Science and Engineering Department, and also our friends who devoted their valuable time and helped us in all possible ways towards successful completion of this project. We thank all those who have contributed either directly or indirectly towards this project.

Lastly, we would also like to thank our families for their unyielding love and encouragement. They always wanted the best for us and we admire their determination and sacrifice.

Date:18/11/2018

Roll No.	Name	Signature
401503008	Brahmrita Singh	
401503009	Chinmaya Garg	
401503015	Kushagra Sharma	
401553002	Jashan Sadioura	

TABLE OF CONTENTS

LIST OF FIGURES

An efficient access control embedded system based on face recognition is very important for a large range of commercial and security applications. Many countries are gradually adopting smart home security control systems [1], [2]. The most important part of any home security system is accurately identifying visitors who enter and leave through the door [3], [4]. An entrance guard can be managed using passwords, RFID sensors, finger prints and face recognition methods [5]. Face recognition is probably the most natural way to perform biometric authentication of human beings. Additionally, it is the second most popular biometric trait, after fingerprints [6]-[8]. Very few researchers have implemented the face recognition techniques in an embedded system for real time applications. Most of the systems are using a principle component analysis (PCA) algorithms [9]-[12] for face recognition on hardware platform for its simplicity and dimensionality reduction [13]-[17].

Wireless technologies like radio frequency identification (RFID), ultra-wide band (UWB), and ZigBee [18] etc. are also used in access control systems.

1.1 Project Overview

1.1.1 TECHNICAL TERMINOLOGY

The project revolves around using Open Source Computer Vision library on a python background interfaced with a 5 MP Pi Camera, a Raspberry Pi, a lock module or a servo motor whichever is being used as a locking-unlocking mechanism. Pi is also referred as Raspberry Pi and the PiCam is the Raspberry Pi camera.

1.1.2 PROBLEM STATEMENT

The problem of efficient and reliable house access is being solved here. Many a times, people are holding stuff or not capable of using both their hands at the time but we need to allow access into the house. The project tries to cater to situations where a person is using biometric authentication to unlock his or her house.

1.1.3 GOAL

To develop a system that works without the need of an individual every time and is made keeping in mind the unavailability of the physical presence of a human at home.

1.1.4 SOLUTION

Implementation of an engaging home security system with the biometric verification using facial recognition.

1.2 NEED ANALYSIS

In the present scenario of smart houses most of the focus is given to the interior of the house i.e. how well the lights work, how one can control the different household utilities through their phones and/or tablets, but little focus has been given to home access system.

The ones who have developed such systems have been charging mind-boggling prices for these facilities and these facilities get outdated very often, with the new technologies emerging very fast. Whatever be the case there is always a presence of an individual required for these so called independent home access systems to work. We are trying to develop a system that works without the need of an individual every time and is made keeping in mind the unavailability of the physical presence of a human at home.

1.3 RESEARCH GAPS

Face detection and recognition are important for many reasons and thus most computer vision algorithms are dedicated to the task of facial feature analysis and recognition such as identifying the age, gender and emotions of different faces despite variations in appearances. This is an open area of research and deep learning once again is currently out performing previous approaches in terms of reliability and accuracy.

One thing to note here is that for most face detection algorithms faces are not tracked but the detection algorithm is run on each frame from a video or streaming camera. The trick is to have computationally efficient algorithms repeated 30

times a second for a 30 frames per second video stream. Optical flow and motion or tracking algorithms are rarely used in face-detection-videos.
Viola-Jones face detection approach is probably the fastest to date, it is still used in digital cameras for detecting faces for things like autofocus and lighting adaptations so that faces are visible. The other approach using Local Binary Patterns (LBP) is also based on adboost algorithm for feature selection. The problem with these approaches is the large number of false positives and are mainly limited to face detection and not recognition, though for basic applications this in not a very big problem.

The more recent approaches to face detection and recognition are based on detecting facial landmarks i.e. nose, mouth, right eye and left eye. This makes for a robust detection pipeline for faces that are not properly aligned such as partial profile faces. This is not very robust though and maybe affected by severe pose changes but this approach is far better than a single sliding window approach. The best thing here is to train several Convolution Neural Networks (CNN) for detecting different facial landmarks and combine the results in the output network.

The other approach is probably the best performing and is based on a novel combination of 3D matching/alignment and deep learning. The face is converted into a 3D model by some sophisticated algorithms and based on the 3D model the algorithm performs a lot of normalization such as normalizing the pose of the face through piecewise affine warping before feeding the result to a nine layer deep neural network that extracts a deeper facial representation

In conclusion none of these approaches are perfect or near human level facial perception, though deep Face claims to be closing the gap. Using deep neural nets for the task of face detection and recognition might be slow on most hardware especially mobile devices thus the Viola-Jones approach might be employed for the task of face detection and only invoke the deep neural net classifiers on detection windows.

1.4 PROBLEM DEFINITION AND SCOPE

The problem of efficient and reliable house access is being solved here.

Let's explain the above scenario through an example. Suppose you go outside and there is no one in the house. With the traditional locking method you would lock the house. But with this facial recognition you just have to use your biometric identification.

The purpose of intelligent home access control system is to ease the process of home access and to create a convenient and easy-to-use application for people in our household, trying to enter the house. The system is based on a deep learning model and Principal Component Analysis(PCA). We will have a database containing the faces of the people that are allowed in the house. Above all, we hope to provide a comfortable user experience along with the best pricing available at the prototype stage.

1.5 ASSUMPTIONS AND CONSTRAINTS

The assumptions and certain things that we have taken in account for in the project are:

Constraints:

The constraints related to this project are:

- Scope:
  - Module design.
  - Establishment of test modules.
  - Separate module interconnection.
  - Portable device which is easy to carry.
- Quality:
  - Camera: 2-5 Megapixels.
  - Ram- 1 GB.
  - Facial detection module with an accuracy, greater than 75%.
  - Efficient algorithms.

- Schedule:

- All of the work is completed in the given timeline with a maximum delay of 4 to 5 days.

- Budget:
  - The minimum amount required by us is 8 thousand INR.
- Resource:
  - The following modules are available to us, given the budget constraint:
    - Raspberry Pi.
    - Camera.
    - Power source.
    - Efficient System.
- Risk:
  - Will to tolerate potential losses of up to 20% of the budget.
  - Individual module's risk.
  - Connection and integration of a large number of modules which would finally ensure the public safety.

Dependencies:

Given that the project fulfils all the requirements and passes all the constraints, there are certain assumptions which have been made for the project to proceed and to be finished successfully:

- We get the funds required by us on time to start the project.
- We will get all the resources, required by us.
- We get six months of time period for completing the project.
- All the group members finish their work on time.
- We get a working and space efficient platform to train the model.
- We get proper dataset to train the model.
- All the models would be configured and work properly.
- There isn't any communication barrier between the user and the device.

1.6 APPROVED OBJECTIVES

The approved objectives as discussed under the guidance of Dr. R.K. Sharma and the first panel evaluation are:

i.) The hardware based implementation of an independent smart home access control system that will work under the following case:

Case: The system would work under proper power availability and lightening conditions in which the face is to be recognized. Under low lighting and from a distance from camera the face is not recognized.

1.7 METHODOLOGY USED

The proposed system is a wireless access control system designed and developed for smart home environment. The paper proposes a Raspberry Pi based door access control and home security system through OpenCV based Haar Cascade. The system identifies the visitor's presence, captures and transfers the image to be verified.

1.8 PROJECT OUTCOMES AND DELIVERABLES

This project presents the design and the implementation of an interactive home security system with the OpenCV measurement and control systems. Replacing PC with low-cost single chip processor which can make administrators to get parameters of different remote devices and send control information to the field equipment at any time through Internet.

The project is divided into several modules:

a.) **Face Recognition Module**: Principal Component Analysis technique, effectively and efficiently represents pictures of faces into its Eigen-face components. It reduces data dimensionality by performing a covariance analysis between factors. When applied on conditions, PCA will explore correlations between samples or conditions. If we consider an image as a point in a very high dimensional space, the principal components [22] are essentially the Eigen-vectors of the covariance matrix of this set of face images, which Turk and Pentland termed the Eigen-face [23]. Each individual

face can then be represented exactly by a linear combination of Eigen-faces, or approximately, by a subset of "best" Eigen-faces, i.e. those that account for the most variance within the face database characterized by its Eigen-values.

b.) **Lock Module**: Lock module includes a servo module, a control circuit or an electromagnetic lock. A 5V-DC circuit can be designed to operate the lock mechanism. The electromagnetic lock has been controlled by the Raspberry Pi.

1.9 NOVELTY OF WORK

The system has been developed indigenously in house with the help of Open Source Computer Vision library. The OpenCV environment comes with face detection algorithms and have been modified with facial recognition algorithms. The next phase of the project that is based n deep learning for faster and more secure facial recognition provides novelty for the work.

CHAPTER 2 - REQUIREMENT ANALYSIS

2.1 LITERATURE SURVEY

Shows the various analyses and research made in the field of your interest and the results already published, taking into account the various parameters of the project and the extent of the project.

2.1.1 Theory Associated With Problem Area

The concept of home automation has been discussed for a long time. But with the new emerging of technology and services, people's expectations of what a home should do or how the services should be provided at home has changed a lot during the course of time, and so has the outlook of home automation systems. If we look at different home automation systems over time, they have always tried to provide efficient, convenient, and safe ways for home inhabitants to access their homes. Irrespective of the change in user requirements, advancement of technology, or change of time, the role of a home automation system has remained the same.

From an engineering point of view, a home can be broken down into the "Six S's" as specified by Brand [28] and given in Figure 1 below, along with who has access to each "S". Home automation systems mainly deal with the last "S's," namely Service, Space Plan, and Stuff. A study [29] showed that in addition to home automation technology and devices, a modern home relies on three to seven services or companies to provide them with infrastructure support like Internet, telephone, electricity, gas, etc. Another study [30] done on different homes showed that people choose the "Site" of the home based on factors like the availability of uninterrupted power, high speed Internet, etc., excluding other factors like property prices and neighbors, which are beyond the scope of this work. The study also showed that a typical home environment handles a plethora of "Services," so many of these services will have to share the resources of the home. The availability of wireless communication nowadays has helped with the "Space Plan" and improved the aesthetics of the modern home. Moreover, home inhabitants add, remove, and move equipment in their home as they please, so "Stuff" always changes in a home. The work of Greichen [31] discussed some of the early challenges faced by home automation systems. These include high manufacturing costs, high development costs,

high installation costs, additional service and support costs, lack of home automation standards, consumer unfamiliarity with technology, and complex user interfaces.

Moreover, a lot of home automation protocols, communication and interface standards like X10 [32], ZigBee [33], LonTalk [34], and CEBus [35] were defined overtime. All these factors have been addressing the challenges and concerns of early home automation systems, which lead to the popularity and wide acceptance of automated homes. The study done by Brush et al. [36] discusses the main problems in modern home automation systems: the high overall cost of the system, intangibility due to integration of different devices into the home automation system, lack of reliable devices at home, complex user and device interactions, and reliance on skilled consultants. All these factors lead to poor manageability and lack of convincing security.

In Figure given below the different "S" of home security systems are given.

Six S's and how often they change	Meaning	Who has accessibility
SITE (Fixed)	This is the geographical setting, location, and the legally-defined lot, which boundaries and context outlast generations of ephemeral buildings.	Civil Engineers Architects Builders
STRUCTURE (30-300 yrs)	The foundation and load-bearing elements are perilous and expensive to change, so people don't. They are the buildings. Structural life ranges from 30 to 300 years.	Builders Painters
SKIN (20-30 yrs)	Exterior surfaces now change every 20 years or so, to keep up with fashion, technology, or for repair.	Builders Painters
SERVICES (20-30 yrs)	These are the working guts of a building: communications wiring, electrical wiring, and plumbing. Buildings are demolished early if their outdated systems are too embedded to replace easily.	Service Providers Plumbers Electricians Inhabitants
SPACE PLAN (3-30 yrs)	The interior layout – where walls, ceilings, floors, and doors go. Turbulent spaces can change every 3 years or so; exceptionally quiet homes might wait 20-30 years.	Designers Painters Inhabitants
STUFF (Continual)	Chairs, desks, phones, pictures, kitchen appliances, lamps, hairbrushes; all the things that move around daily or monthly. Furniture is called "mobilia" in Italian for good reason.	Inhabitants

FIGURE 1: The above image shows the six "S".

A lot of research has gone into automating the home [37], [38], making it accessible via the Internet [39] or mobile phones [40], [41], saving energy [42], technology assisted living for senior citizens [43], and security [44]. Existing research only addresses and proposes defenses against normal intrusion attempts at home, and doesn't consider the risk of intrusion from sophisticated or tech-savvy criminals. Our work mainly focuses on the security aspect of home automation.

We first discuss how the perception of security has changed in modern home automation systems, then focus on various challenges in the field from a security point of view.

2.1.2 Existing Systems and Solutions

"The tasks of a modern security system include identifying an intruder trying to gain access to the home, alerting the homeowner about the intrusion or intrusion attempt, preventing the intruder from gaining access to the home, and gathering or collecting evidence regarding the intrusion so that the perpetuators can be brought to justice."

Actors perform the appropriate actions on the environment as directed by the user or any other party. Improvements in Wireless Sensor Actor Networks are certainly a contributing factor in the popularity of smart homes. Combining Ubiquitous Computing, Wireless Sensor Actor Networks and the popularity of the Internet has allowed designers, engineers, and researchers to come up with efficient methods to allow home inhabitants to access and control each and every aspect of their home, including the environment. Commonly used technologies and networks for home automation have many vulnerabilities, as discussed by Karlof and Wagner [45].

They consider various routing attacks on wireless sensor networks (WSNs). This includes Sinkhole attacks, Selective Forwarding attacks, Sybil attacks, and Cloned ID attacks. In 2006, Hu et al. [46] detected an important attack on wireless networks called a Wormhole attack in which the attacker records data packets in the network at one location, tunnels them to another location, and retransmits them to the network. This attack can be carried out even if all communications in the network are done with confidentiality and integrity using IP sec in 6LoWPAN. Data packet integrity, device authenticity, key establishment, and encryption standards are specified in almost all wireless encryption protocols these days. In 2011, Wright et al. [47] showed how a ZigBee or 802.15.4 wireless networks can be hacked using replay attacks [48]. During re-flashing, the new key is sent in plain text over the air. An attacker can take advantage of this and sniff for encryption keys in plain text, inject, decode, and alter data packets to manipulate a device's operations. In 2013, Fouladi and Ghanoun [49] demonstrated a vulnerability in Z-Wave door locks, which gave the attacker full access without proper authorization.

In 2013, Oluwafemi et al. [50] showed how a simple device in a home, such as a fluorescent lamp (CFL), which is connected to a home automation network or Internet could be manipulated to cause physical harm (shattered glass, fire outbreak, mercury poisoning) to a home's inhabitants. Moreover, lights fluctuating at certain frequencies

could be very dangerous for people with photosensitive epilepsy [51]. When a home automation network is connected to the Internet, there is the possibility that an attacker could gain control of switches and dimmers along with devices plugged into the power outlets. Researchers also discussed the presence of some well-known vulnerabilities in home automation systems, such as Cross Site Scripting (XSS). They were able to embed persistent JavaScript in the log pages of one of the products. The researchers also observed that in some home automation systems, every communication between the homeowner and home automation system, both from within the home network and over the Internet, is done in clear text (over the Internet HTTP is used instead of HTTPS).

This allows an attacker to attach itself on the communication and gather legitimate login credentials. In some home automation systems, a user is authenticated using an authentication cookie, which is not associated with any session ID or expiration time frame, so if an attacker could steal this authentication cookie from a legitimate user and include it in their browser session, they could bypass the authentication page altogether. In an attempt to capture the home automation market companies and designers gave little importance to security.

But for homes it is different. The home is a place where everybody is supposed to feel safe and secure. Even the slightest doubt that a home could be compromised can have a serious psychological impact on its inhabitants. We have to give a broader explanation or meaning to the term “intruder” in our definition when we combine homes with the Internet and ubiquitous computing, also considering the number of devices used in home automation today and their vulnerabilities. In traditional homes, intruders could only steal or threaten a home if they are in physical proximity to the home.

Our concept of intruder has to evolve from the traditional sense in order to account for device vulnerabilities. A lot of research has gone into identifying and preventing such intruders by using alarms, infrared sensors, or contact sensors, but very little work has gone into identifying and preventing technologically-skilled intruders.

2.1.3 Research Findings for Existing Literature

The research done by the group has been tabulated below in table 1.

S. No.	Roll Number	Name	Paper Title	Tools/ Technology	Findings	Citation
1	401503015	Kushagra Sharma	Home Automation Methodologies Analyzed from a Security Standpoint Context-aware Home Security Systems	Context Aware Computing.	Creates privacy issues since the system is keeping a track of the surrounding.	[54], [55]
2	401503015	Kushagra Sharma	Bluetooth-based Home Security System	Using a cell phone that used a bluetooth host	The system was bluetooth based and so the remote access to the system was only possible within 10 meters.	[60], [61]
3	401503015	Kushagra Sharma	Central Controller-based Home Security System	Using a central controller to connect and control home devices.	If the central controller was lost or damaged the whole system became useless.	[58], [59]
4	401503015	Kushagra Sharma	GSM or Mobile-based Home Automation System	Using a GSM module to connect different devices.	If the cellular services were down or the	[41]

					signal quality was low the system would not work.	
5	401503015	Kushagra Sharma	SMS-based Home Security System	Using SMS to communicate with devices.	It has the same problem as GSM or home based Automation System.	[63]
6	401503015	Kushagra Sharma	GPRS-based Home Automation System	Using a GPRS module to communicate with devices.	It has the same problem as GSM or home based Automation System.	[40], [65]
7	401503009	Chinmaya Garg	Security considerations for secure and trustworthy smart home system in the IoT environment		Security Requirements and functions of smart home system in the IoT nature.	[29]
8	401503009	Chinmaya Garg	Door lock system via web application	Raspberry Pi Motion Sensor Limit Switch Stepper Motor Door Lock	Commands like lock cannot be done if the limit switch i.e. door is not closed fully and hence threatens the safety and	[30]

					security.	
9	401503009	Chinmaya Garg	Research Directions for the Internet of Things		What can be done with IOT and how to do it step by step.	[31]
10	401503009	Chinmaya Garg	Design and implementation of a smart home control system.		It mention that the version of internet protocol (IP) still used IPv4 and most addresses provided by IPv4 have been used, is not possible to provide static IP address for each device. To construct the complete environment of IOT the network address shortage will be a big issue	[36]
11	401503009	Chinmaya Garg	Smart Home-Control and Monitoring System Using Smart Phone		Due to the popularity of the Internet is growing up thus any problems of the Internet	[37]

					are also happening	
12	401503009	Chinmaya Garg	The Implementation of Smart Electronic Locking System Based on Z-Wave and Internet	Raspberry Pi Z-Wave wireless transmission Mobile devices	In case a device was included and moved afterwards to a new position, this particular device can only be controlled by the remote control if it is in direct range. Otherwise the communication will fail	[38]
13	401553002	Jashanpreet Singh Sadioura	Smart Home-Control and Monitoring System Using Smart Phone		Due to the popularity of the Internet is growing	[20],
14	401553002	Jashanpreet Singh Sadioura	An efficient image processing based technology using Raspberry Pi			[36] [37]
15	401553002	Jashanpreet Singh Sadioura	The Implementation of Smart Electronic Locking System Based on Z-Wave and Internet	Raspberry Pi Z-Wave wireless transmission Mobile devices	In case a device was included and moved afterwards to a new position,	[50] [51]

					this particular device can only be controlled by the remote control if it is in direct range. Otherwise the communication will fail	
16	401553002	Jashanpreet Singh Sadioura	Devices Smart electric Surveillance	Electric energy utilization is the type of energy consumption that uses power. Electricity utilization is the actual power demand made on current electricity supply.		[45]
17	401553002	Jashanpreet Singh	Bluetooth-based Home Security System	Using cell phone as a bluetooth host		[60]
18	401553002	Jashanpreet Singh Sadioura	Comparative study on various systems based ob raspberry technology			[35]
19	401503008	Brahmrita Singh	Face Detection and Recognition using Viola-Jones	PCA, ANN and Voila-Jones algorithm	Combination of PCA and feed forward	[19]

			algorithm and Fusion of PCA and ANN		neural network produces better results	
20	401503008	Brahmrita Singh	A Review Paper on Face Recognition Techniques	Comprehensive Literature Review	PCA is better for small sample size, LDA for large sample size, SVM is better for generalization and ICA provides better results than PCA	[22]
21	401503008	Brahmrita Singh	A Study on Facial Feature Extraction and Facial Recognition Approaches	SIFT, SURF, PCA and LDA	SIFT is invariant to scale, rotation, affine transformation, noise and occlusion and SURF matches the key points between altered image and each database image	[25]
22	401503008	Brahmrita Singh	Geometrical and Visual Feature Quantization for 3D Face Recognition	Naïve bayes, multilyae perceptron and random forest classifiers	By applying bag of features approach and varying	[34]

					histogram levels, the effectiveness of facial recognition was improved	
23	401503008	Brahmrita Singh	A Comparative Study on Various State of the Art Face Recognition Techniques under Varying Facial Expressions	DCT, overlapping DCT and moments	Overlapping DCT is best for recognising faces under slight facial expression variations and CSM is best for higher varying degrees of facial expressions	[30]
24	401503008	Brahmrita Singh	GPU Based Face Recognition System for Authentication	GPU with CUDA	GPU gives far better results than CPU due to its fast computational capability	[31]

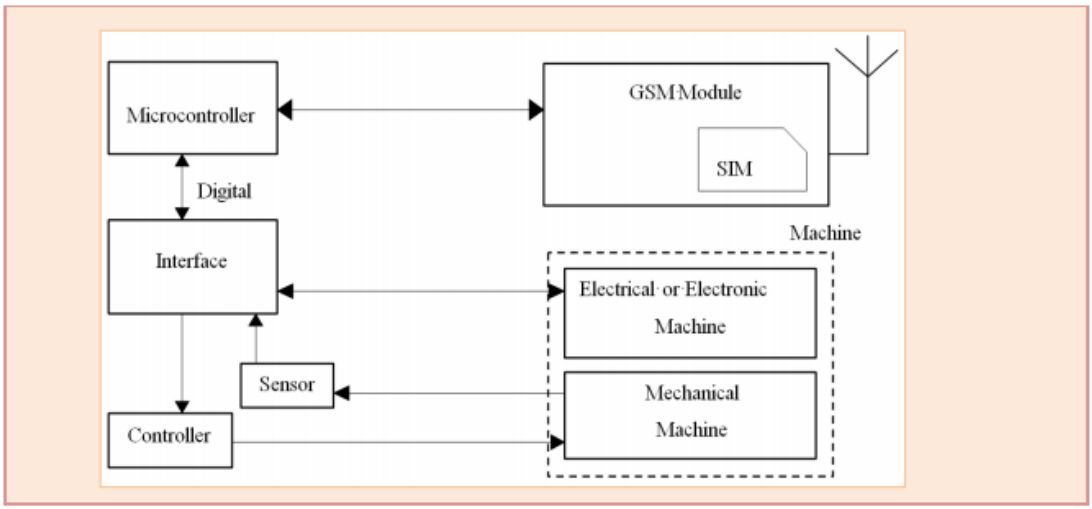
Table 1: Research Assessment Done by the Students

2.1.3.1 Home Automation Technologies Analyzed from a Security Standpoint

Context-aware Home Security Systems

We can't expect the user to be security conscious every time he or she accesses their home from the outside. This brings in new security vulnerabilities to the home front. Understanding the context of a particular action by the user could go a long way in improving a home's security. The work of Dey [54] defines context as "Any

information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves." In this home automation system, the system tries to be aware of the context in which a user understands a decision. Predicting the location of a user inside the home adds to defining the context.



Mobile-based home automation from the work of *A. Alheraish* [14].

Figure 2: Mobile Home Automation Framework

2.1.4 The Problem That Has Been Identified

The unavailability of a low cost secure and reliable system. The systems that are presently available have drawbacks as listed above and are much more expensive than our system.

2.1.5 Survey of Tools and Technologies Used

The tools used by this system are(Hardware) :
1.Face Recognition Algorithms

2.Pi Camera Module

3.Electronic Lock Module

Tools Used(Software):

1.Python

2.Raspberry Pi

3.Raspian Software

2.2 STANDARDS

The standards for the Raspberry Pi are given as:

Product	SoC	Speed	RAM	USB Ports	Ethernet	Wireless/Bluetooth
Raspberry Pi Model A+	BCM2835	700MHz	512MB	1	No	No
Raspberry Pi Model B+	BCM2835	700MHz	512MB	4	Yes	No
Raspberry Pi 2 Model B	BCM2836/7	900MHz	1GB	4	Yes	No
Raspberry Pi 3 Model B	BCM2837	1200MHz	1GB	4	Yes	Yes
Raspberry Pi 3 Model B+	BCM2837	1400MHz	1GB	4	Yes	Yes

Our Raspberry Pi uses a 1.2Ghz Quad Core 64 bit Arm cortex-A53 CPU, has 1 GB RAM, integrated 802.11n, and blue tooth 4.1.

2.3 SOFTWARE REQUIREMENTS SPECIFICATION

The certain dependencies and requirements have been analyzed in this section.

2.3.1.1 Purpose

The purpose of this document is to build an embedded home access system that uses facial recognition to ease the process of home security and provides reliable authentication.

2.3.1.2 Intended Audience and Reading Suggestions

The project is a prototype of an intelligent home access control system. This will be implemented under the guidance of Dr. R. K. Sharma. The projects intends to be used in households so that the traditional way of locking and unlocking the door can be replaced by an automated and more reliable authentication process.

2.3.1.3 Project Scope

The purpose of intelligent home access control system is to ease the process of home access and to create a convenient and easy-to-use application for people in our household, trying to enter the house. The system is based on a deep learning model which uses Principal Component Analysis(PCA). We will have a database supporting the faces of the people that are allowed in the house. Above all, we hope to provide a comfortable user experience along with the best pricing available at the prototype stage.

2.3.2 Overall Description

The Intelligent home access system does the following:
1) FACIAL RECOGNITION: The system recognizes the face of the people that are allowed to enter the house.

2.3.2.1 Product Perspective

Our Methodology consists of the following steps:

a. Using a Feature Detection Technique

A feature detection technique namely Harr Cascade will be used for the purpose of detecting an object in an input image extracted from the live feed using a camera. These types of models are provided by several organizations like Matlab, Google, OpenCV e.t.c. These models have already been trained using thousands of images of different objects each. Forming these types of models for such huge data requires a lot of time as well as high processing power based systems.

So, these feature detection technique are going to be used and further images of more number of different objects would be added depending on the need.

b. Object recognition from the input images

An image is extracted from the frame by frame live feed provided by a camera and read using OpenCV. This image is further passed to the model which detects objects present in the image. If an object's class is recognized, a rectangular frame is formed around the detected object and the accuracy by which the given object's class is recognized is given out as output along with the class name. A given threshold value for the accuracy of the class detected would be set to increase the efficiency of the model.

SEQUENCE DIAGRAM

A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams are typically associated with use case realizations in the Logical View of the system under development. Sequence diagrams are sometimes called event diagrams or event scenarios.

A sequence diagram shows, as parallel vertical lines (lifelines), different processes or objects that live simultaneously, and, as horizontal arrows, the messages exchanged between them, in the order in which they occur. This allows the specification of simple runtime scenarios in a graphical manner.

From the term Interaction, it is clear that the diagram is used to describe some type of interactions among the different elements in the model. This interaction is a part of dynamic behavior of the system.

This interactive behavior is represented in UML by two diagrams known as Sequence diagram and Collaboration diagram. The basic purpose of both the diagrams are similar.

Sequence diagram emphasizes on time sequence of messages and collaboration diagram emphasizes on the structural organization of the objects that send and receive messages.

2.3.2.2 Product Features

The product features are given in the E R Diagram given in this section:

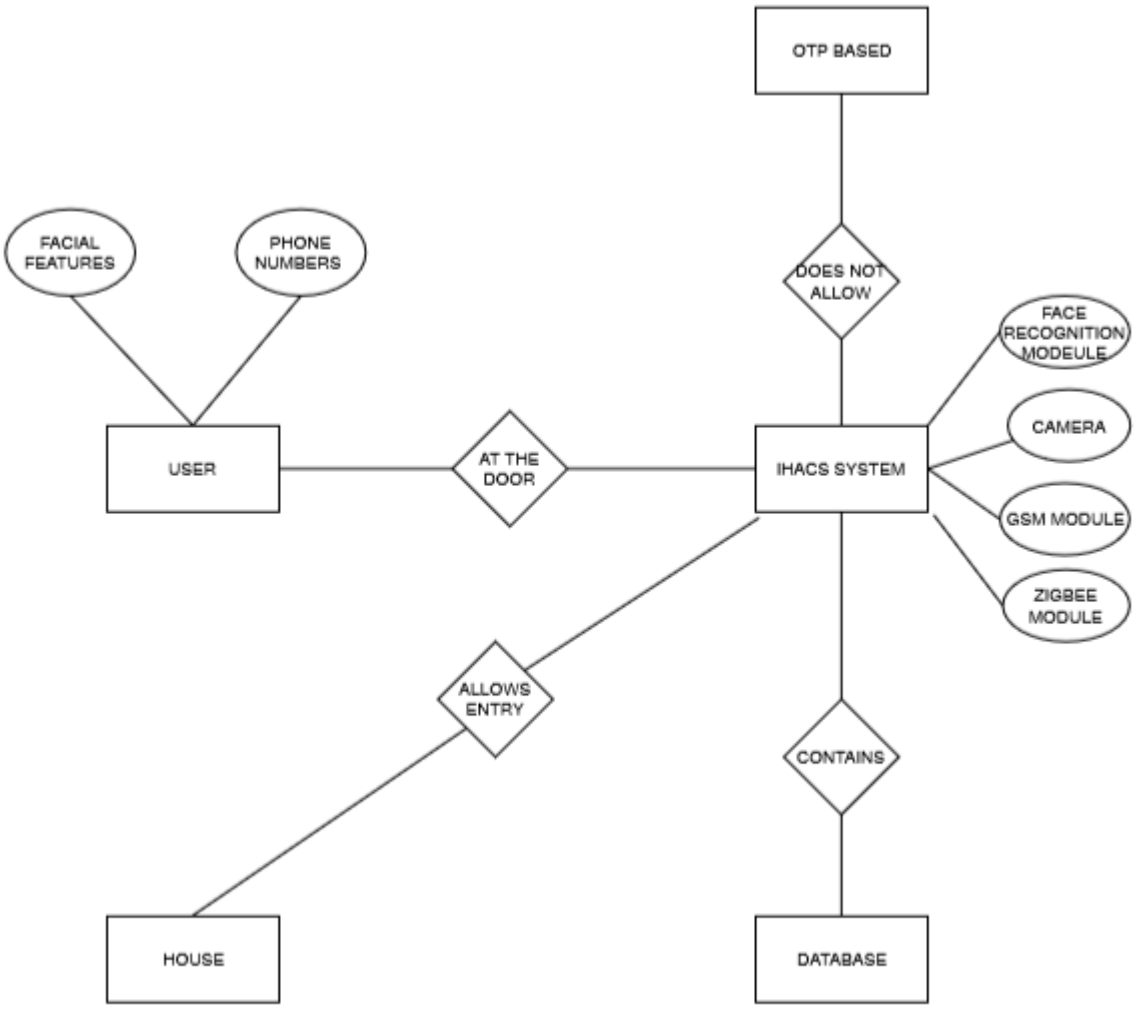


Figure 3: The figure shows the ER representation

USER CLASS AND CHARACTERSTICS

There are two classes of users that interact with the system:

1) The users whose face is in the database maintained: The users whose facial features are maintained in the database can enter the house without any worry, their faces will be detected and the door will automatically get unlocked.

2) The users whose face is not in the database: The users whose face is not in the database but still wish to enter the house can pursue this through OTP based entry.

2.3.3 External Interface Requirements

The system will be installed at the door so that the faces can be detected. The working environment will be outside the door so it should be prone to all the weather conditions .

2.3.3.1 Hardware Interfaces

Following will be used for hardware interfaces:

- Raspberry Pi
- Camera
- Servo Motor
- Switch

2.3.3.2 Software Interfaces

Operating environment for the iHACS system is as listed below.

- database
- GSM/server system
- Operating system: Windows.
- database: SQL+ database
- platform: Python

2.3.4 Other Non-functional Requirements

In systems engineering and requirements engineering, a **non-functional requirement**(NFR) is a requirement that specifies criteria that can be used to judge the operation of a system, rather than specific behaviors.

2.3.4.1 Performance Requirements

- **AVAILABILITY:** The system should be available at all times of the day.
- **CORRECTNESS:** The system should be able to predict all the faces with specified accuracy.
- **MAINTAINABILITY:** The system should be maintainable for a certain time.
- **USABILITY:** The system should be easy to use.

2.3.4.2 Safety Requirements

- Proper and strong connections
- Proper Wiring
- Quality wires and materials
- Camera lens not to be touched
- Provide appropriate voltage

2.3.4.3 Security Requirements

Security systems need database storage just like many other applications. However, the special requirements of the security market mean that vendors must choose their database partner carefully.

2.4 COST ANALYSIS

The cost involved for various components used are:

a. Raspberry Pi board (1 unit)= Rs. 3000

b. LED (2 units) = 2*50=Rs. 100

c. Bread Board= Rs. 300

d. USB connectors (5 units)=5*50=Rs. 250

e. Raspberry Pi Camera=Rs. 800

f. Relay driver circuit (1 unit)= Rs. 150

g Electromagnetic lock (1 unit)= Rs. 1200

2.5 RISK ANALYSIS

The risk analysis of the project has been done below:

2.5.1 RISK IDENTIFICATION

The risk that can be identified related tour project can be tabulated as follows:

Risk Register	
ID	Description
1.	Software Error
2.	Hardware Error
3.	Loose Connections
4.	Wrong Detection
5.	No Detection
6.	Attack by Intruder

2.5.2 QUALITATIVE ANALYSIS

The qualitative assessment of the project has been done below:

Risk Register					
ID	Description	Probability	Impact	Score	Priority
4.	Wrong Detection	2	3	6	1
5.	No Detection	1	3	3	2

2.5.1 RISK MANAGEMENT PLAN

Software Error

There might come some bugs that we are currently unaware of. The software is well-tested and reliable till date but as we know nothing is perfect so there might come some bugs after full-fledged implementation. It will cost us time, money, and quality. This will be solved by the trained professionals by re-installing the software and finding the root of the problem.

Hardware Error

Supply of input voltage might damage the hardware. Impact on hardware may damage it. Feeding it to much training pics for one person that other family members pics cannot get uploaded by filling up all the memory. It will cost us resources that are

time and money. This will be solved by the trained hardware engineers by repairing or changing the hardware whichever is necessary and finding the root of the problem.

Loose Connections

The connections will be firm and tight but there might be a chance that connections may get loose. It may occur by a strike or poor manufacturing. It might also happen if someone willingly pulled them off. It will cost us resources that are time and money. This will be solved by the trained hardware engineers by fixing or changing the connection wires whichever is necessary and finding the root of the problem.

Wrong Detection

This might happen sometimes if the model is not trained properly. Input image for training might not be of good quality. There might be dust on camera not giving camera the clear image. It will be solved by providing a new dataset to be trained.

No Detection

It might be due to some software issue. Camera might be blocked will be the main reason or some serious issue or bug in the algorithm might be the reason. Restarting system should solve the problem but if it still persists and continues to occur at intervals. This will be a very serious problem which will be dealt by the software professionals.

CHAPTER 3 – METHODOLOGY ADOPTED

3.1 INVESTIGATIVE TECHNIQUES

Experimental

1. HAAR Cascaded was used for facial recognition. It is a filter based image segmentation technique which uses a set of filters. The filters are divided into dark and light filters in which sum of black pixels are subtracted from black pixels.

2. Similar facial recognition algorithms that have been developed using machine learning and deep learning have been developed but they put a solid impact on the hardware required.

3.2 PROPOSED SOLUTION

The proposed solution is a wireless access control system designed and developed for smart home environment. Raspberry Pi based door access control and home security system through PiCam based technology. The system identifies the visitor's presence, capture and transfers the image through to the database automatically to the home owner to recognize the visitors. It has a variety of features such as energy efficiency, intelligence, low cost, portability and high performance.

3.3 WORK BREAKDOWN STRUCTURE

The project has been broken into different modules as discussed above and at the end all of them will be interfaced as per the dataflow of the project.

3.4 TOOLS AND TECHNOLOGIES USED

The methods and tools used by this system are given in this section.

Methods Used:

The project is divided into modules:

The main modules involved in the project are:

1.Face Recognition

2.PiCam

3.Electronic Lock Module

Tools Used:

1.Python

2.Raspberry Pi

3.Raspian Software

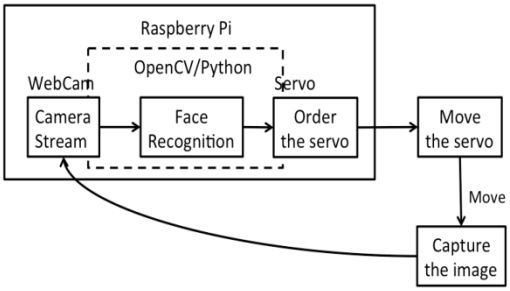
4.A camera to capture real time images

CHAPTER 4 - DESIGN SPECIFICATIONS

4.1 SYSTEM ARCHITECTURE

The remote monitoring and controlling of the embedded equipments over the Internet can be mechanized by following certain network architectural design strategies and applying communication standards. The data transmission of camera is done directly. The virtual home security System is a software developed in python. All communication and instructions are checked for security and safety, in the virtual environment, before implementation in the real home environment.

The Raspberry Pi unit and the camera are installed in a home. If any visitors arrive, the Raspberry Pi sends the appropriate details .The system architecture has been given below in the figure.



Face Recognition Module

Principal Component Analysis technique, effectively and efficiently represents pictures of faces into its eigen face components. It reduces data dimensionality by performing a covariance analysis between factors. When applied on conditions, PCA will explore correlations between samples or conditions. If we consider an image as a point in a very high dimensional space, the principal components are essentially the eigenvectors of the covariance matrix of this set of face images, which Turk and Pentland termed the eigen face . Each individual face can then be represented exactly by a linear combination of eigen faces, or approximately, by a subset of "best" eigen faces - those that account for the most variance within the face database characterized by its eigen values.

Lock Module

Lock module includes a servo module or a control circuit and an electromagnetic lock. A 5v DC circuit has been designed to operate the electromagnetic lock. The electromagnetic lock has been controlled through the control circuit. When the command received is “open”, the control circuit will deenergize the lock to open the door. Else the lock gets energized to close the door.

SYSTEM COMPONENTS

The system is divided into various modules that form the components of the system. The modules are namely

1.Face Recognition Module

2.Lock Module

DATA MODEL

The data model represents how data goes about in the designed product. The data flow in our project has been represented below in Figure 4.

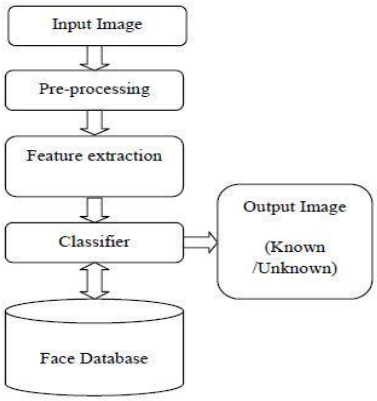


Figure 4: Flow of Data in the System.

4.2 DESIGN LEVEL DIAGRAMS

A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams are typically associated with use case realizations in the Logical View of the system under development. Sequence diagrams are sometimes called event diagrams or event scenarios.

A sequence diagram shows, as parallel vertical lines (lifelines), different processes or objects that live simultaneously, and, as horizontal arrows, the messages exchanged between them, in the order in which they occur. This allows the specification of simple runtime scenarios in a graphical manner.

From the term Interaction, it is clear that the diagram is used to describe some type of interactions among the different elements in the model. This interaction is a part of dynamic behavior of the system.

This interactive behavior is represented in UML by two diagrams known as Sequence diagram and Collaboration diagram. The basic purpose of both the diagrams are similar.

Sequence diagram emphasizes on time sequence of messages and collaboration diagram emphasizes on the structural organization of the objects that send and receive messages.

Purpose of Interaction Diagrams

The purpose of interaction diagrams is to visualize the interactive behaviour of the system. Visualizing the interaction is a difficult task. Hence, the solution is to use different types of models to capture the different aspects of the interaction.

Sequence and collaboration diagrams are used to capture the dynamic nature but from a different angle.

The purpose of interaction diagram is :

- To capture the dynamic behavior of a system.

- To describe the message flow in the system.
- To describe the structural organization of the objects.
- To describe the interaction among objects.

We have already discussed that interaction diagrams are used to describe the dynamic nature of a system. Now, we will look into the practical scenarios where these diagrams are used. To understand the practical application, we need to understand the basic nature of sequence and collaboration diagram.

The main purpose of both the diagrams are similar as they are used to capture the dynamic behavior of a system. However, the specific purpose is more important to clarify and understand.

Sequence diagrams are used to capture the order of messages flowing from one object to another. Collaboration diagrams are used to describe the structural organization of the objects taking part in the interaction. A single diagram is not sufficient to describe the dynamic aspect of an entire system, so a set of diagrams are used to capture it as a whole.

Interaction diagrams are used when we want to understand the message flow and the structural organization. Message flow means the sequence of control flow from one object to another. Structural organization means the visual organization of the elements in a system.

Interaction diagrams can be used −

- To model the flow of control by time sequence.
- To model the flow of control by structural organizations.
- For forward engineering.
- For reverse engineering.

4.3 USER INTERFACE DIAGRAMS

The images related to the connection of the setup steps and flow of data in the project are given in figure 5 :

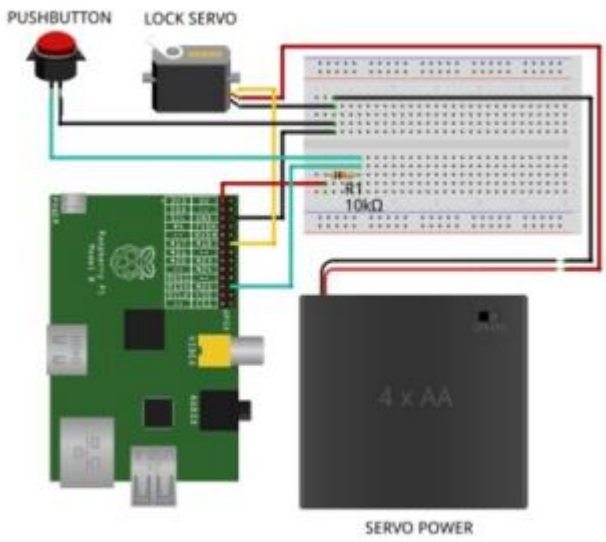


Figure 5: Context Diagram

Data flow in this framework:

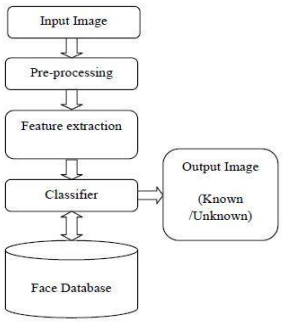


Figure 6: This shows the flow of data in the project

4.4 SYSTEM SCREENSHOTS

The screenshots generated during the testing of the model are given below in figure 7.

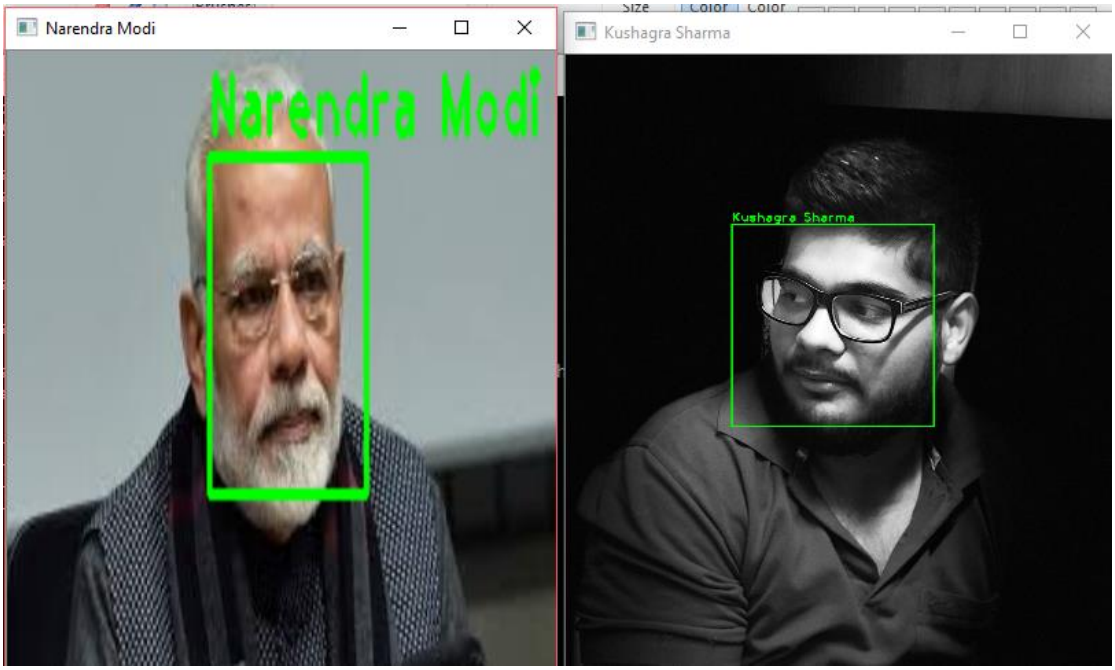


Figure 7: System Screenshots

CHAPTER 5 – IMPLEMENTATION AND EXPERIMENTAL RESULTS

5.1 EXPERIMENTAL SETUP (OR SIMULATION)

The experimental setup is just an in-house environment where there is proper lighting and enough headspace so that the camera can capture the images of the face of the entrant in an easy manner. The Raspberry Pi camera is good but does not perform well under low lighting often missing faces or recognizing certain part of a face turning the system redundant in low light.

Under the ideal condition the system will detect the face and unlock the door.

5.2 EXPERIMENTAL ANALYSIS

5.2.1 DATA

The data is collected in the form of images. For each user a test case folder is generated. The model has two sets of folders. One for positive images and one for negative images. The negative folders contain a set of images that will train the model to not recognize these images. The positives folder will consist of a set of folders one for each user. Each of these folders will contain a set of 10-15 images so that the model can learn the features of the face it has to recognize.

5.2.2 PERFORMANCE PARAMETERS

The lone performance parameter that the team will be using would be the accuracy with which the model is recognizing the face. The accuracy will be in percentage and a number will be displayed along with the bounding box when the face is recognized.

5.3 TESTING PROCESS

5.3.1 Test Plan

The test plan consists of different scenarios that the system can work under. Generally speaking whenever a door based system is designed, it is done in a way that it can undergo through different weather conditions. But due to limited budget and the capability restriction of the Raspberry Pi we will test the model under indoor conditions. The test plan includes making a well lit camera area so that the camera can capture images well. It also should allow head movement and the camera should be placed at eye level height so that it can capture the image.

The test plan includes to test all the modules separately i.e. the camera module and the lock module and then the system as a whole package.

5.3.1.1 Features to be tested

The team will be testing the feature detection capabilities of the model and how well the model recognizes face under different lightening and angles. Sometimes as it happens there is a tilt in the face or there is head movement. This is a challenge for the system so the team will test the model under different facing angles and lighting conditions. The model is trained using different looks of the owner so that whenever the user is wearing spectacles or changes his look the system can recognize it.

5.3.1.2 Test Strategy

The test strategy includes testing the face recognizing capabilities under different lightening conditions and different facing angles.

5.3.1.3 Test Techniques

Test Techniques are not very well defined in different cases. What was required was a eye level height camera mount along with proper lightening.

5.3.2 Test Cases

The test cases do not include some exclusive cases. The team just needs to train the model on a varied set of images of each user. Also the test cases are defined by physical conditions under which the system is tested rather than software issues.

Test Case 1: Under well lighted conditions with straight face.

Under this test case the face is put in front of the camera under well lit conditions. A straight face is applied rather than tilting the head

Test Case 2: Under dimly lit conditions with straight face.

Under this condition the model is tested under dimly lit conditions with a straight face. The model recognizes the face based upon the lighting conditions. The test results will we mentioned below.

Test Case 3: Under well lit conditions with a tilted face.

Under this case there is well lit area but the face is tilted . The model recognizes the face until a certain tilt angle but after that the system stops recognizing the face.

Test Case 4:Under dimly lit conditions with a tilted face.

This is the worst case of all the test cases The system faces the most difficulty in recognizing the face under this condition and the accuracy with which the face is recognized is also very low.

5.3.3 Test Results

Under the first two test cases when the face is kept straight in front of the camera the system recognizes the face with above average accuracy. But under dim lighting there is a threshold under which the system recognizes the face.

Under the nest two test cases when the face is tilted the accuracy drops down but with the well lit the system is recognizing the face but under the dimly lit conditions the system is not able to recognize the face at all.

5.4 RESULTS AND DISCUSSIONS

Results show that the system performs well under near ideal conditions with a straight face and well lit conditions but with a tilted face and under dimly lit conditions both the accuracy and the number of time the face is recognized drops. Thus we get to know that we need to have an eye level camera mount and good lighting so that the system works with good accuracy and faster than usual.

5.5 INFERENCES DRAWN

The inferences drawn are that we need to gave a well lit room where the camera module is mounted. We need to find a reliable power source and an eye level camera mount to make the system work ideally.

5.6 VALIDATION OF OBJECTIVES

Thus the objectives which were previously defined are fulfilled i.e. our face module and the lock module both work as intended.

CHAPTER 6: CONCLUSIONS AND FUTURE DIRECTIONS

6.1 CONCLUSIONS

The conclusion is that we are using biometric verification (facial verification) to provide an alternative to traditional locking system using the Raspberry Pi that will result in an efficient, low power consuming and reliable home access authentication system.

6.2 ENVIRONMENTAL, ECONOMIC AND SOCIETAL BENEFITS

The Raspberry Pi is made under the green revolution technologies so it leaves a minimal carbon footprint as compared to other commercially available SoCs. We are also using low power SoC so the energy consumption for this 24*7 running system is minimized.

The society needs to evolve with the evolving technologies. We should use a more reliable and hassle free technology is it is available and this system does so.

6.3 REFLECTIONS

The project opened the team to new evolving technologies such as machine learning and python. Overall the project can be termed as an exciting learning opportunity that enhanced our skill set as computer science students.

6.4 FUTURE WORK

The future work intentions are to use an faster Soc coupled with more secure camera system i.e. we can use Infrared Camera system that are currently being used in phones. it is one of the most secure facial recognition system and requires a high level of technical knowledge to implement.

CHAPTER 7: PROJECT METRICS

7.1 CHALLENGES FACED

The most difficult challenge for the group was using the Raspberry Pi and then using the GPIO pins to implement the lock mechanism. The Raspberry Pi generally works with a screen but since the team was not having a screen the Raspberry Pi had to be used along with a Xming software . The IP needed to be known and every time the connection was made we needed to re-obtain the changed IP. Connecting to the Raspberry Pi and then establishing the connection was a very difficult task.
The gpio library with which the lock mechanism was operated was very hard to crack and kept on throwing errors again and again.

7.2 RELEVANT SUBJECTS

The relevant subjects for the project were machine learning and an advanced knowledge of the Raspian operating system and the Raspberry Pi. The project seemed achievable at first but when we delved deep into the project it turned out to be pretty challenging..

7.3 INTERDISCIPLINARY KNOWLEDGE SHARING

The team had to learn a lot of Electronics for the Raspberry Pi .Raspberry Pi is an independent SoC and its usage is entirely different from a traditional system. The team had to learn a lot of stuff that delved into electronics to learn about Raspberry Pi.

7.4 PEER ASSESSMENT MATRIX

The rating of the student are as follows

		Evaluation of			
		Kushagra	Chinmay	Jashan	Bhramrita
Evaluation By	Kushagra	4	4	3	3
	Chinmay	5	5	4	4
	Jashan	5	5	4	4
	Brahmrita	5	5	4	4

7.5 ROLE PLAYING AND WORK SCHEDULE

The work schedule of the project was very much affected by the team members being of the dual Degree MBA program. Due to prior commitments and other subjects going on the project as always being completed on the deadline.
The different roles played by each team member is:
Kushagra: Concerned with developing the code of the facial recognition module.
Chinmay: Concerned with developing the Locking Mechanism GPIO code.
Jashan: Concerned with the testing of the modules.
Brahmrita: Concerned with the hard ware aspect.

7.6 STUDENT OUTCOMES DESCRIPTION AND PERFORMANCE INDICATORS (A-K MAPPING)

SO	Description	Outcome
1	Identify the constraints, assumptions and models for the problems.	YES, we understood the constraints the hardware provided us for such a project and amended the changes that were needed.
2	Use appropriate methods, tools and techniques for data collection.	We used the techniques and tools that in spite of limited computing power would help us in achieving the desired results.
3	Can understand scope and constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability.	The product helps us to understand that low power consumption is what is needed right now. Since our product is based on the
4	Fulfill assigned responsibility in multidisciplinary teams.	The whole team performed as a unit and did all the work that required multiple attention to different domain.
5	Can play different roles as a team player.	The team performed as a unit to take up the task of assembling
6	Showcase professional responsibility while interacting with peers and professional communities.	The group performed well and spoke softly with all the mentors that were present during the evaluations
7	Deliver well-organized and effective oral presentation.	The group to the best of their abilities performed the task of giving presentations.

7.7 BRIEF ANALYTICAL ASSESSMENT

In a brief it can be said that the project proved to a very good learning experience for the group. The project involved going out of the way from the course syllabus and techniques. We had very good experience with building things and making them work for ourselves. It's good to see how product development takes place and how we could learn to work in a team, cover each other's work and at the end come out with a product that works.

Q1. What sources of information did your team explore to arrive at the list of possible Project Problems?
Ans) The group first took the project of signature analysis but finding the project in the list of previously attempted project rejected them**.** Then we checked our several resources that included Google searches , projects on Adafruit.com and other

resources. We found that this project was interesting and upon the consultation of the mentor we decided to work upon it.

Q2. Did the project demand demonstration of knowledge of fundamentals, scientific and/or engineering principles? If yes, how did you apply?
Ans) The project required knowledge of machine learning and feature extraction techniques that are used for age and object detection and recognition. The group as a whole learned these techniques and put them to use in the project.

Q3. How did your team shares responsibility and communicate the information of schedule with others in team to coordinate design and manufacturing dependencies?
Ans) The main medium of communication between the groups were WhatsApp group and emails. All the documents and other necessary documents were shared through email. To distribute the processes involved the team met often between the semester to discuss the work that was distributed and how the progress was going.

Q4.What resources did you use to learn new materials not taught in class for the course of the project?
Ans) Often time the knowledge required was not taught in the class . For this we required extra resources which the internet provided. Most of the time stack overflow and other online resource website provided the data and resources. If then also there was any problem we would report to our mentor sir and ask for suggestions that could be useful.

Q5. Does the project make you appreciate the need to solve problems in real life using engineering and could the project development make you proficient with software development tools and environments?
Ans) In the long run every programmer is related to some product development and wants to learn how a certain product is perceived and then how we go about it. Through this project we learned how to go about this project and how we can develop a certain product on a timeline. So it was a learning experience for us to get to develop this product.

REFERENCES

[1] Jinsoo Han, Chang-Sic Choi, Ilwoo Lee, "More efficient home energy management system based on ZigBee communication and infrared remote controls", *IEEE Transactions on Consumer Electronics* , vol. 57, no. 1, pp. 85-89, February 2011.

[2] H. Erdem, A. Uner, "A multi-channel remote controller for home and office appliances," *IEEE Transactions on Consumer Electronics*, vol. 55, no. 4, pp. 2184-2189, November 2009.

[3] Yuksekkaya, B. Kayalar, A.A. Tosun, M.B. Ozcan, M.K. Alkar, "A GSM internet and speech controlled wireless interactive home automation system, "*IEEE Transactions on Consumer Electronics*, vol. 52, no. 3, pp. 837-843, Aug. 2006.

[4] Chia-Hung Lien, Ying-Wen Bai, Ming-Bo Lin, "Remote-Controllable Power Outlet System for Home Power Management", *IEEE Transactions on Consumer Electronics*, vol. 53, no. 4, pp. 1634-1641, Nov. 2007.

[5] S. Vernon, S.S. Joshi, "Brain–Muscle–Computer Interface: Mobile Phone Prototype Development and Testing, " *IEEE Transactions on Information Technology in Biomedicine*, vol.15, no.4, pp.531,538, July 2011.

[6]M. Faundez-Zanuy, "Are inkless fingerprint sensors suitable for mobile use?", *IEEE Aerospace and Electronic Systems Magazine*, Vol. 19, No. 4, pp. 17-21, April 2004.

[7]M. IFaundez-Zanuy, "Technological evaluation of two AFIS systems", *IEEE Aerospace and Electronic Systems Magazine*, Vol. 20, No. 4, pp. 13-17, April 2005

[8]M. Faundez-Zanuy, "Privacy issues on biometric systems", *IEEE Aerospace and Electronic Systems Magazine,* Vol. 20, No. 2, pp. 13-15, February 2005.

[9] P. B. Saurabh, D.S.Chaudhari, "Principal Component Analysis for Face Recognition", *International Journal of Engineering and Advanced Technology*, vol. 1, pp. 91-94, 2012.

[10] S. M. Prakash, C. J. Kalpna, "Face Recognition Using PCA", *International Journal of Artificial Intelligence Knowledge Discovery*, vol. 1, pp. 25-28, 2011.

[11] A. M. Martinez, A. C. Kak, "PCA versus LDA" , *LOS ALAMITOS*, pp. 228-233, 2001.

[12] J. Mazanec, "Support vector machines, PCA and LDA in face recognition", *Journal of Electrical Engineering* , vol. 59, pp. 203-209, 2008.

[13] K. H. Pun, "A face recognition embedded system", *Biometric Technology for Human Identification II,* vol. 5779, 2005.

[14] R. Ibrahim, Z. M. Zin, "Study of automated face recognition system for office door access control application" , *IEEE 3rd International Conference in Communication Software and Networks (ICCSN)*, Beijing, China, 2011, pp. 132- 136.

[15] W. Shimin, Y. Jihua, "Research and implementation of embedded face recognition system based on ARM9", *IEEE Conference Proceedings*, 2010, pp. 2618-2621.

[16] H. T. Ngo, "A flexible and efficient hardware architecture for real time face recognition based on eigen face", *IEEE Computer Society Annual Symposium Proceedings in VLSI*, 2005, pp. 280-281.

[17] G. F. Zaki, "Using the hardware/software co-design methodology to implement an embedded face recognition/verification system on an FPGA", *IEEE Conference Proceedings*, 2007, pp. 459-462.

[18] Il-Kyu Hwang, Jin-Wook Baek, "Wireless access monitoring and control System based on digital door lock", *IEEE Transactions on Consumer Electronics*, Vol. 53, Nov 2007, pp. 1724-1730.

[19] Maik Schmidt. Raspberry Pi. *A Quick Start Guide. Dallas*, Texas: The Pragmatic Bookshelf, 2012, pp. 11-42.

[20] Mo Guan, Minghai Gu, "Design and implementation of an embedded web server based on ARM", *IEEE International Conference on Software Engineering and Service Sciences (ICSESS)*, 16-18 July 2010, pp. 612-615.

[21] Hong-TaekJu, Mi-Joung Choi and James W. Hong “An efficient and lightweight embedded Web server for Web-based network element management” *International Journal of Network Management*, pp. 261 – 275, Oct 2000.

[22] T.F. Karim, M.S.H. Lipu, M.L. Rahman, F. Sultana, "Face recognition using PCA-based method", *IEEE International Conference on Advanced Management Science (ICAMS)*, vol. 3, Singapore, 9-11 July 2010, pp. 158-162.

[23] M. Turk, A. Pentland, " Eigenfaces for Recognition*", Journal Cognitive Nero-science*, 1991.

[24] *XBee-PRO RF Module. Digi Int. Inc., Hopkins, MN, USA.* [Online]. Available: http://www.digi.com, accessed Jun. 15, 2013.

[25] *IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks,* IEEE Standard 802.15.4, 2003.

[26] Rhydo Technologies, "SIM900 GSM/GPRS RS232 Modem – User Manual", Dec, 2011.

[27] N.M. Barnes, N.H. Edwards, D.A.D. Rose, and P. Garner, "Lifestyle monitoring technology for supported independence," *Computer Control Engineering*. vol. 9, pp. 169-174, Aug. 1998.

[28]S. Brand," How Buildings Learn: New York", Viking, 1994.

[29] R.E. Grinter, N. Ducheneaut, W.K. Edwards, M. Newman, "The work to make a home network work", *Ninth European Conference on Computer-Supported Cooperative Work (ECSCW 05)*, pp. 469-488, 2005.

[30] M. Chetty, J.Y. Sung, R.E. Grinter, "How Smart Homes Learn: The Evolution of the Networked Home and Household," *Lecture Notes in Computer Science, vol. 4717*, pp. 127-144, 2007.

[31] Greichen, J.J., "Value based home automation or today's market," *IEEE Transactions on Consumer Electronics*, vol. 38, no. 3, , Aug. 1992, pp.34-38.

[32] "The X10 Specification," X-10 (USA) Inc., 1990.

[33] "ZigBee Specifications," ZigBee Alliance, version 1.0 r13, Dec. 2006.

[34] "LonTalk Protocol Specification Version 3.0," Echelon Co, 1994.

[35] “EIA-600 CEBus Standard Specification”, *EIA*, 1992.

[36] A.J. Bernheim Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, C. Dixon, “Home automation in the Wild: Challenges and Opportunities,” , *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Vancouver , 2011, pp. 2115-2124.

[37] K. Madhuri, B. L. Sai, B. S. Sirisha, “A Home Automation System Design Using Hardware Descriptive Tools,” *International Journal of Engineering Research & Technology*, vol. 2, no. 7, Jul. 2013.

[38] E.M.C Wong, “A Phone-Based Remote Controller for Home and Office Automation,” *IEEE Transactions on Consumer Electronics*, vol. 40, Feb. 1994, pp.28-34.

[39] A. ElShafee, K.A. Hamed, “Design and Implementation of a WiFi Based home automation System,” *World Academy of Science, Engineering and Technology*, vol. 6, 2012.

[40] M. Danaher, D. Nguyen, “Mobile Home Security with GPRS”, *8th International Symposium for Information Science*, Oct. 2002.

[41] A. Alheraish, “Design and Implementation of Home Automation System,” *IEEE Transactions on Consumer Electronics*, vol. 50 , Nov. 2004, pp.1087-1092.

[42] V. Singhvi, A. Krause, C. Guestrin, James H. Garrett Jr., H. Scott Matthews, “Intelligent Light Control using Sensor Networks,” *Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems*, 2005, pp. 218-229.

[43] A. Gaddam, “Development of a Bed Sensor for an Integrated Digital Home Monitoring System,” *IEEE International Workshop on Medical Measurements and Applications*, pp. 33-38, May 2008.

[44] U. Saeed, S. Syed, S.Z. Qazi, N. Khan, A. Khan, M. Babar, “Multi-advantage and security based home automation system”, *Fourth UK Sim European Symposium on Computer Modeling and Simulation (EMS)*, Nov. 2010, pp.7-11.

[45] C. Karlof, D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures”, *Ad Hoc Networks*, vol. 1, pp. 293–315, 2003.

[46] Y. Hu, A. Perrig, D. Johnson, “Wormhole attacks in wireless networks”, *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 370–380, Feb. 2006.

[47] J. Wright, “Practical ZigBee Exploitation Framework”, *Toorcon*, Oct. 2011.

[48] Z. Feng, J. Ning, I. Broustis, K. Pelechrinis, S.V. Krishnamurthy, M. Faloutsos, “Coping with Packet Replay Attacks in Wireless Networks,” *8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pp. 368-376, Jun. 2011.

[49] B. Fouladi, S. Ghanoun, “Security Evaluation of the Z-Wave Wireless Protocol,” Black Hat USA, Aug. 2013.

[50] T. Oluwafemi, S. Gupta, S. Patel, T. Kohno, “Experimental Security Analyses of Non-Networked Compact Fluorescent Lamps: A Case Study of home automation Security,” *Workshop on Learning from Authoritative Security Experiment Results*, pp. 13 – 34, Oct. 2013.

[51] A. Verrotti, D. Trotta, C. Salladini, G. Corcia, G. Latini, R. Cutarella, F. Chiarelli, “Photosensitivity and epilepsy: a follow-up study,” *Developmental Medicine & Child Neurology*, vol. 46, May 2004, pp. 347-351.

[52] T. Hyun-Jin Kim, L. Bauer, J. Newsome, A. Perrig, J. Walker, “Access Right Assignment Mechanisms for Secure Home Networks,” *Journal of Communications and Networks*, vol. 13, pp. 175-186, 2011.

[53] Michelle L. Mazurek, “Access Control for Home Data Sharing: Attitudes, Needs and Practices,” *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 645-654, 2010.

[54] Dey, A. K., “Understanding and Using Context,” *Personal and Ubiquitous Computing*, vol. 5 , pp. 4-7, Feb. 2001.

[55] B. Schilit, N. Adams, R. Want, “Context-Aware Computing Applications,” *WMCSA '94 Proceedings of the 1994 First Workshop on Mobile Computing Systems and Applications*, pp. 85-90, 1994.

[56] V. Bellotti, K. Edwards, “Intelligibility and Accountability: Human Considerations in Context Aware Systems,” *Human-Computer Interaction*, vol. 16, issue 2, pp. 193-212, Dec. 2001.

[57] Stephen S. Intille, “Designing a Home of the Future,” *IEEE Pervasive Computing*, vol. 1, no. 2, pp. 76-82, Apr. 2002.

[58] S.-M. Tsai, P.-C. Yang , S.-S. Wu , S.-S. Sun, “A Service of Home Security System on Intelligent Network,” *IEEE Transactions on Consumer Electronics*, vol. 44, no. 4, pp. 1360-1366, Nov. 1998.

[59] K. Atukorala, D. Wijekoon, M. Tharugasini, I. Perera, C. Silva, “SmartEye - Integrated solution to home automation, security and monitoring through mobile phones,” *Third International Conference on Next Generation Mobile Applications, Services and Technologies*, NGMAST '09, pp. 64-69, Sep. 2009.

[60] N. Sriskanthan, F. Tan, A. Karande, “Bluetooth based home automation system,” *Microprocessors and Microsystems, Elsevier, vol. 26*, pp. 281-289, 2002.

[61] H. Kanma, N. Wakabayashi, R. Kanazawa, H. Ito, “Home Appliance Control System over Bluetooth with a Cellular Phone,” *IEEE Transactions on Consumer Electronics*, vol. 49 , no. 4, pp.1049-1053, Nov. 2003. Article (CrossRef Link)

[62] M. Ryan, “Bluetooth: With Low Energy comes Low Security,” WOOT'13 *Proceedings of the 7th USENIX conference on Offensive Technologies*, pp. 4-4, 2013.

[63] M. Sikandar, H. Khiyal, A. Khan, E. Shehzadi, “SMS Based Wireless Home Appliance Control System (HACS) for Automating Appliances and Security,” *Issues in Informing Science & Information Technology*, vol. 6, Jan. 2009.

[64] A. R. Delgado, R. Picking, V. Grout, “Remote-Controlled home automation systems with Different Network Technologies,” *Centre for Applied Internet Research (CAIR)*, University of Wales, 2009.

[65] Bing-Fei Wu, Hsin-Yuan Peng, Chao-Jung Chen, “A Practical Home Security System via Mobile Phones,” *TELEINFO'06 Proceedings of the 5th WSEAS international conference on Telecommunications and informatics*, pp. 299-304, 2006.

APPENDIX B

The plagiarism report for the project file is given below in Figure 8:

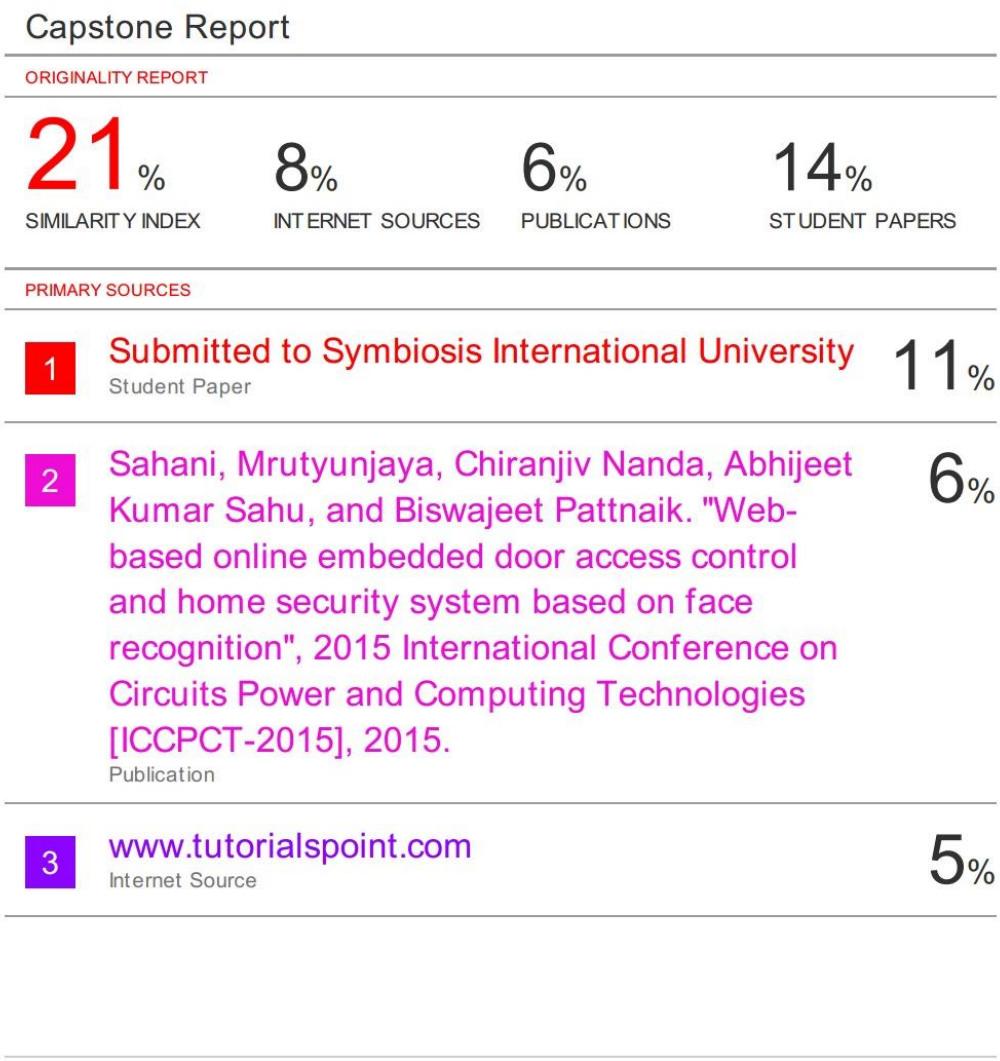


Figure 8: Plagiarism Report