An Intelligent Vision System for monitoring Security and Surveillance of ATM

CS18L1 Project

12150820	**CSU14118**	**Balanarayanan Kartha V**
12150852	**CSU14143**	**Prasanth M P**
12150913	**CSU14154**	**Shweta Ann Jacob**
12150920	**CSU14159**	**Thanvi Rabia**

B. Tech Computer Science & Engineering

Department of Computer Engineering
Model Engineering College
Thrikkakara, Kochi 682021
Phone: +91.484.2575370
http://www.mec.ac.in
hodcs@mec.ac.in

April 2018

Model Engineering College Thrikkakara
Department of Computer Engineering

C E R T I F I C A T E

This is to certify that, this report titled **An Intelligent Vision System for monitoring Security and Surveillance of ATM** is a bonafide record of the work done by

12150820	**CSU14118**	**Balanarayanan Kartha V**
12150852	**CSU14143**	**Prasanth M P**
12150913	**CSU14154**	**Shweta Ann Jacob**
12150920	**CSU14159**	**Thanvi Rabia**

Eighth Semester B. Tech. Computer Science & Engineering students, for the course work in **CS18L1 Project**, which is the second part of the two semester project work, under our guidance and supervision, in partial fulfillment of the requirements for the award of the degree, B. Tech. Computer Science & Engineering of **Cochin University of Science & Technology**.

Guide

Sheena Y
Assistant Professor
Computer Engineering

Coordinator

Manilal D L
Associate Professor
Computer Engineering

Head of the Department

Manilal D L
Associate Professor
Computer Engineering

April 12, 2018

Acknowledgements

This project would not have been possible without the kind support and help of many individuals. We would like to extend our sincere thanks to all of them. First of all, We would like to thank our esteemed Principal, Prof. (Dr.) V.P Devassia, for his guidance and support in maintaining a calm and refreshing environment to work in and also for providing the facilities that this work demanded. We are highly indebted to our Project Coordinator, Dr. Manilal D L, Associate Professor and Head of the Department, Dr. Priya S, Associate Professor for their guidance, support and constant supervision throughout the duration of the work as well as for providing all the necessary information and facilities that this work demanded. We would like to thank our Project Guide, Sheena Y for her support and valuable insights and also for helping us out in correcting any mistakes that were made during the course of the work. We offer our sincere gratitude to all our friends and peers for their support and encouragement that helped us get through the tough phases during the course of this work. Last but not the least, we thank the Almighty God for guiding us through and enabling us to complete the work within the specified time.

Balanarayanan Kartha V

Prasanth M P

Shweta Ann Jacob

Thanvi Rabia

Abstract

This project proposes an automated system to increase the security and surveillance of ATM kiosks. Due to the increase of robbery in ATM kiosks, it is important to employ an automated surveillance system to protect and secure the ATM machine from threats. Currently, a camera attached with the ATM unit, records and transmits the video feed to the main server of the bank. Around the clock, this manual surveillance utilizes a lot of bandwidth for transmission. There is waste of memory and late response to emergency situation. Consequently, early detection of the situation is necessary to take preventive measures against an ongoing burglary. This project makes it possible to detect whether a person is wearing a mask or not. The proposed system is also capable of counting the number of people present inside the ATM kiosk and generate a warning signal, thereby removes a constant human supervision, reducing the storage of unnecessary video feed and transmitting only an anomalous situation, a faster response to a threat as soon the system detects the threat. Also, it generates a warning when a person enters the ATM frequently in a short span of time.

Contents

List of Figures

Chapter 1

Introduction

In this modern era of automation many scientific advancements and inventions have taken place to save labor, increase the accuracy and to ameliorate our lives. One such system is an Automated ATM Surveillance System. The purpose of this project is to develop a system to improve the existing surveillance system in ATM's thereby increasing the security. The proposed project automates the ATM surveillance thereby removing the need for around the clock surveillance and decreasing the response time. Using this system it is possible to detect anomalous activities. The system is able to detect whether the person inside the kiosk is wearing a mask and if the same person has entered the ATM kiosk multiple number of times. It also detects the number of people that is present inside the kiosk at a given time. In case of suspicious behavior, an alert is sent to the bank security officials.

An Automated ATM Surveillance System which is developed using face recognition, generally consists of Image Acquisition, Database development, Face detection followed by Face recognition. This product is eliminates the need for around the clock manual surveillance.

This aims at automating the whole procedure by using a combination of face detection and recognition algorithms to detect suspicious activities in an ATM kiosk and to produce an alert. Once implemented, it can save time,and reduce the chances of error.

1.1 Proposed Project

- Automated ATM Surveillance System that adopts Human Face Recognition (HFR).
- Involves the process of extracting key features from any facial image of a person present inside the ATM kiosk.
- Produces an alert if more than four people are present inside the ATM kiosk.
- Produces an alert if a person wearing a mask enters the ATM kiosk.
- Produces an alert if a person stays inside the ATM kiosk for more than 20 minutes.
- Produces an alert if a person enters the ATM kiosk more than four times in an interval of one hour.

1.1.1 Problem Statement

Around the clock, the manual surveillance of ATMs utilizes a lot of bandwidth for transmission. There is waste of memory and late response to emergency situation. Consequently, early detection of the situation is necessary to take preventive measures against an ongoing burglary.

1.1.2 Proposed Solution

This project proposes an automated system to increase the security and surveillance of ATM kiosks.This project makes it possible to detect suspicious behavior in an ATM kiosk produce an alert. This system eliminates the need for around the clock manual surveillance. It detects whether a person is wearing a mask or not. The proposed system is also capable of counting the number of people present inside the ATM kiosk and generate a warning signal, thereby removes a constant human supervision. It reduces the need for storage of unnecessary video feed, transmitting and storing only in case of an anomalous situation. This enables a faster response to threats as soon the system detects the threat. Also, it generates a warning when a person enters the ATM frequently in a short span of time.

A Web based interface is also provided where authorized bank officials can log in to view the live video feed from the camera inside the ATM kiosk. A log of all the alerts generated along with a timestamp is also available. This alert log can be reviewed by the bank officials in the future.

Chapter 2

System Study Report

2.1 Literature Survey

Several Face detection and recognition algorithms have been designed till date.Each of them have their ups and downs.The table below shows a detailed comparison of the advantages and disadvantages of some popular methods.

2.1.1 An Intelligent Vision System for monitoring Security and Surveillance of ATM

Advantages	Disadvantages
Eliminates the need for around the clock surveillance	The lighting condition and the background of the localized environment have been assumed to be constant
Cheap and simple in terms of hardware and complexity	High negative detection
Requires small database and bandwidth	Requires full view of frontal upright faces
Faster response in an emergency situation	
Shuts down the ATM machine if a threat is detected	

2.1.2 Automatic Video Surveillance for theft detection in ATM machines : An enhanced approach

Advantages	Disadvantages
Faster response time	Requires a large database
Eliminates the need for around the clock surveillance	

2.1.3 Smart ATM Surveillance System

Advantages	Disadvantages
Eliminates the need for around the clock surveillance	High hardware requirements
Faster response time	Expensive
Robust	
Automatic shutter locking mechanism traps the burglars inside the kiosk	
Stability and reliability	

2.1.4 Abnormal Activity Detection for Bank ATM Surveillance

Advantages	Disadvantages
Eliminates the need for around the clock surveillance	Expensive
3D camera provides depth image	Requires constant lighting

2.1.5 Crime Detection and Avoidance in ATM: A New Framework

Advantages	Disadvantages
Overcomes the barrier of manual video surveillance	It has potential for privacy abuse due to identification capabilities.
Detects Multiple person issues	Poor lighting inside the room can reduce the efficiency
Alarm goes off if threat is detected	

2.1.6 Face Occlusion Detection for Automated Teller Machine Surveillance

Advantages	Disadvantages
Eliminates the use of manual video surveillance	The lighting inside the room is considered to be constant
Can detect face occlusion	It has potential for privacy abuse due to identification capabilities
Can detect multiple people through occlusion	Need Complex indoor environment

2.1.7 Image-based Fraud Detection in Automatic Teller Machine

Advantages	Disadvantages
Eliminates the use of manual video surveillance	The lighting inside the room is considered to be constant
Alarm goes off if threat is detected	It has potential for privacy abuse due to identification capabilities
Can detect moving objects	Sometimes erroneous results are obtained

2.1.8 Vision-Based System for Automatic Detection of Suspicious Objects on ATM

Advantages	Disadvantages
It has no detection miss and false alarm	It fails to detect suspicious objects sometimes.
The proposed system increases correctly detected area by 13.21 percentage than the fixed threshold method	Need constant lighting conditions

2.1.9 Smart ATM-Reactive Measures against Physical Threats

Advantages	Disadvantages
With the help of interactive GUI, operators work can become very convenient	Identifying threats using secure codes is complex.
The system is configured to work in real time to solve problems on the fly	

2.2 Proposed System

This project proposes an automated system to increase the security and surveillance of ATM kiosks.This project makes it possible to detect whether a person is wearing a mask or not. The proposed system is also capable of counting the number of people present inside the ATM kiosk and generate a warning signal, thereby removes a constant human supervision, reducing the storage of unnecessary video feed and transmitting only an anomalous situation, a faster response to a threat as soon the system detects the threat. Also, it generates a warning when a person enters the ATM frequently in a short span of time.

Chapter 3

Software Requirement Specification

3.1 Introduction

3.1.1 Purpose

The purpose of this document is to develop a system to improve the surveillance in ATM's thereby increasing the security. This document contains details about the various hardware and software tools used in the project.

3.1.2 Document Conventions

This document follows MLA Format. Bold-faced text has been used to emphasize section and sub-section headings. Highlighting is to point out words in the glossary and italicized text is used to label and recognize diagrams.

3.1.3 Intended Audience and Reading Suggestions

This document is intended for all individuals participating in and/or supervising the project.Readers interested in a brief overview of the product should focus on the rest of Part 3.1 (Introduction), as well as Part 3.2 of the document (Overall Description), which provide a brief overview of each aspect of the project as a whole. Part 3.3 (External Interface Requirements) offers further technical details, including information on the user interface as well as the hardware and software platforms on which the application will run.

Readers interested in the hardware and software requirements should read part 3.4 and for functional requirements they should check part 3.5. Readers interested in the non-technical aspects of the project should read Part 3.6, which covers performance, safety, security, and various other attributes that will be important to users.

3.1.4 Project Scope

This project presents an automated system to increase the security and surveillance of ATM kiosks. Due to the increase of robbery in ATM kiosks, it is important to employ an automated surveillance system to protect and secure the ATM machine from threats. Currently, a camera attached with the ATM unit, records and transmits the video feed to the main server of the bank. Around the clock, this manual surveillance utilizes a lot of bandwidth for transmission. There is waste of

memory and late response to emergency situation. Consequently, early detection of the situation is necessary to take preventive measures against an ongoing burglary.
With an automated surveillance system, it is possible to detect whether a person is wearing a mask or not. The proposed system is also capable of counting the number of people present inside the ATM kiosk and generate a warning signal, thereby removing constant human supervision, reducing the storage of unnecessary video feed and transmitting only an anomalous situation.

3.1.5 Overview of Developers Responsibilities

The developer has to choose a suitable programming methodology that is efficient in order to implement this project. The developer is also responsible for
(a) developing the system,
(b) installing the software on the clients hardware,
(c) conducting any user training that might be needed for using the system, and
(d) maintaining the system for a particular time period after installation

3.2 Overall Description

3.2.1 Product Perspective

Computer Science researchers have already come up with methods for automated methods for ATM surveillance. This product is a replacement for the traditional system of assigning a person to monitor the ATM at all times. It aims at automating the whole procedure by using a combination of face detection and recognition algorithms to identify individuals and mark their attendance.Once implemented, it can save time,and reduce the chances of error.In this product,we are planing to combine the already existing automation methods with face detection to identify if a person entering the ATM has put covered the face and to count the number of people inside the ATM. It also uses various face recognition algorithms. We are also adding a database that stores the faces that we recognize. This database can be used to determine the number of times a person has entered the ATM kiosk during a particular interval.

3.2.2 Product Functions

1. Face recognition : Faces of all the people entering the ATM kiosk are uniquely identified.This is done using the database. When a person enters the ATM face recognition algorithms are applied to find out whether that person has entered the kiosk in the past one hour.

2. Covered face detection : If a person entering the kiosk has covered his face using any means possible an alert is generated.

3. Timeout Detection : If a person continues to linger inside the ATM kiosk, a timeout alert is produced after 20 mmin.

4. No. of people detection : If more than 4 people are present inside the ATM at the same time a Threshold reached alert id issued.

5. Frequency Detection : If a person enters the ATM kiosk more than 4 times in an hour an alert is issued.

6. Alert Issue : The bank officials are notified via an alert in case of suspicious behavior. Each of the predefined situations has an unique alert signal.

7. Alert Log : Bank officials can log in to the web page to view the alert log which contains the type of alert and the time at which the alert was produced.

8. Live Videofeed : The bank officials can log in to the web page to view the live videofeed from the webcam.

3.2.3 User Classes and Characteristics

The application is intended to be used by bank security officials, who may not possess any technical expertise. The user simply needs to have basic knowledge of how to use the system.

3.2.4 Operating Environment

- Server
- Open CV software
- Linux OS
- Python Django

3.2.5 Design and Implementation Constraints

- The analysis of the feed depends on the quality of the camera used.
- The background lighting should be constant.
- Constraints in processing of image and identifying whether that person already exists in the database.
- Sometimes in face recognition, a prerecorded face pattern may not match with the current facial expression.
- A bright image impede the detection of certain set of features of the face. Similarly,a dark image produces low contrast image making it difficult to detect the variation in the intensity level along the face.

3.2.6 User Documentation

This surveillance system does not require any user documentation since it simply detects an anomalous situation and transmits it.

3.2.7 General Constraints

The quality of the video feed obtained decides the efficiency of the system. The background lighting should remain constant.

3.2.8 Assumptions and Dependencies

The person entering the ATM kiosk should be in the field of view while an image is being captured since their detection is impossible otherwise.It is assumed that the picture is properly lit and the faces are detectable.As quality decreases, the accuracy in detection and recognition also decreases.The system is assumed to have enough processing speed to run the detection and recognition algorithms.The application, at the time of running must satisfy the dependencies like the presence of a supported Linux Distribution.

3.3 External Interface Requirements

3.3.1 User Interfaces

The UI will be a web page where the bank officials can log in, view the alert log and the live videofeed from the camera inside the ATM kiosk.

3.3.2 Hardware Interfaces

A CCTV camera is used for face recognition which is used to check whether the person entering the ATM is wearing any mask. If he is covering his face then an alert will be sent to the bank officials.

3.3.3 Software Interfaces

A Database is kept which stores the images captured (in the form of a matrix containing the feature vectors) using face recognition. It must be protected so that the data is not misused. It is also used to check whether the same person enters the ATM again and again within a span of 1 hour and how long the person is inside the ATM.

3.3.4 Communication Interfaces

The only communication is between the data from the camera and the server. It is done with HTTP protocol. HTTP protocol will be used to create the applicatopn layer for the software. FTP protocol is used for the tranfer of files to the server.

3.4 Hardware and Software Requirements

3.4.1 Hardware Requirements

The project needs a CCTV camera. PC or Laptop with minimum 512 Mb RAM and 2GB HDD.The processor must not be sluggish and works well for image processing.

3.4.2 Software Requirements

The project requires

- Ubuntu - 64 bit
- OpenCV

3.5 Functional Requirements

3.5.1 Dataset

The system does not require a dataset initially. AS people enter the ATM kiosk a comprehensive dataset which consists of multiple images of each subject is created dynamically.The system reads training images for each person/subject along with their labels, detect faces from each image and assign each detected face an integer label of the person it belongs.Images of the same person must have the same ID.

Training The dataset prepared is used to train the LBPH recognizer before it is ready to function.

Testing Various sample input images are provided to the system to check the accuracy of its predictions and to make necessary changes if required.

3.5.2 Face Detection

Face detection using Haar feature-based cascade classifiers requires a set of positive and negative images to train the classifier.After that , all relevant features are extracted from it.For each feature extraction , sum of pixels under different chosen rectangles are calculated.. For each feature, it finds the best threshold which will classify the faces to positive and negative.

3.5.3 Face Recognition

With the facial images already extracted, cropped, resized and usually converted to grayscale, the face recognition algorithm is responsible for finding characteristics which best describe the image.The LBPH(Local Binary Pattern) algorithm uses 4 parameters:

- Radius: the radius is used to build the circular local binary pattern and represents the radius around the central pixel. It is usually set to 1.
- Neighbors: the number of sample points to build the circular local binary pattern. Keep in mind: the more sample points you include, the higher the computational cost. It is usually set to 8.
- Grid X: the number of cells in the horizontal direction. The more cells, the finer the grid, the higher the dimensionality of the resulting feature vector. It is usually set to 8.
- Grid Y: the number of cells in the vertical direction. The more cells, the finer the grid, the higher the dimensionality of the resulting feature vector. It is usually set to 8.

3.5.4 Web Interface

A web interface for use by the bank officials.Bank officials can keep track of the alerts issued and monitor the video feed from the camera inside the ATM kiosk.

3.6 Non-functional Requirements

3.6.1 Performance Requirements

Since the product is primarily concerned with face detection and recognition, accurate and fast performance is expected when it comes to processing images.Also, the product should perform upto expected standards under varying conditions like lighting, angle etc. in the input images. The system should able to efficiently access the database to perform various functions.

3.6.2 Safety Requirements

The product should be tolerant to current web based attacks.Software attacks like SQL injection, Cross site scripting etc. should not be able to cause harm to the database or the code.Direct access to the database and the live video feed without proper authentication and authorization should not occur.

3.6.3 Security Requirements

The product should incorporate all basic security checks like password, security questions etc to authenticate users.Sensitive information must be encrypted to ensure maximum security.

3.6.4 Software Quality Attributes

Since the system primarily aims at automating the ATM surveillance system to make it less cumbersome, important qualities it should have are user-friendly interface, faster response time to threats, faster access to the database and high accuracy when it comes to face isolation and recognition.It should also have provisions for viewing the activities inside the ATM.

Chapter 4

System Design

4.1 System Architecture

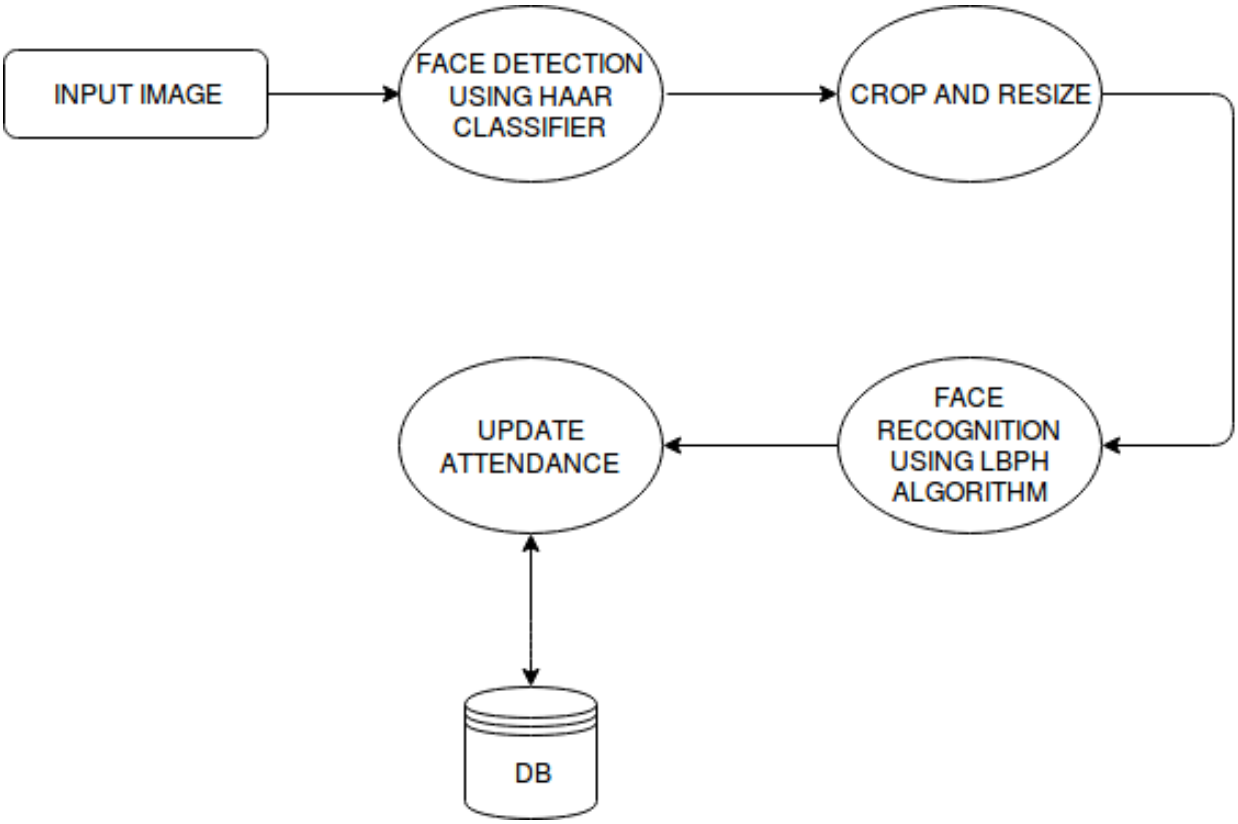


Figure 4.1: System Architecture

The methods based on image processing techniques for illumination problem commonly attempt to normalize all the face images to a canonical illumination in order to compare them under the identical lighting conditions.For this purpose, the images in RGB format is converted to grayscale. Grayscale is a range of shades of gray without apparent color. The darkest possible shade is black,

which is the total absence of transmitted or reflected light. The lightest possible shade is white, the total transmission or reflection of light at all visible wavelength s.
Three methods can be used.The lightness method averages the most prominent and least prominent colors: (max(R, G, B) + min(R, G, B)) / 2.The average method simply averages the values: (R + G + B) / 3.The luminosity method is a more sophisticated version of the average method. It also averages the values, but it forms a weighted average to account for human perception. Humans are more sensitive to green than other colors, so green is weighted most heavily. The formula for luminosity is 0.21 R + 0.72 G + 0.07 B.

4.2 Input Design

In an information system, input is the raw data that is processed to produce output. During the input design, the developers must consider the various input devices being used in the system. Therefore, the quality of system input determines the quality of system output. Well designed input forms and screens have following properties

- It should serve specific purposes effectively such as storing, recording, and retrieving the information.
- It ensures proper completion with accuracy.
- It should be easy to fill and straightforward.
- It should focus on users attention, consistency, and simplicity.

Objectives for Input Design

- To design data entry and input procedures
- To reduce input volume
- To design source documents for data capture or devise other data capture methods
- To design input data records, data entry screens, user interface screens, etc
- To use validation checks and develop effective input controls

4.3 Database Design

Attributes	Description	Type
User Id	Gives a unique user id for each person.	Integer
Alert	Stores the alert issued,if any for the corresponding variable.	Varchar
Timestamp	Gives the time at which the corresponding alert was issued.	Datetime

Figure 4.2: Log Table

Attributes	Description	Type
Name	Stores a string that uniquely identifies each person entering the kiosk.	Varchar
Image	Stores the path to the folder containing the images of that person.	Varchar
Frequency	Stores the number of times a person enters the ATM in an hour.	Integer
Timestamp	Gives the time in which the user first entered the kiosk and was entered into the database.	DateTime

Figure 4.3: Users Table

Chapter 5

Libraries and Packages Used

OpenCV : OpenCV (Open Source Computer Vision Library) is released under a BSD license.It has C++, Python and Java interfaces and supports Windows, Linux, Mac OS, iOS and Android. OpenCV was designed for computational efficiency and with a strong focus on real-time applications. Written in optimized C/C++, the library can take advantage of multi-core processing.The library has more than 2500 optimized algorithms, which includes a comprehensive set of both classic and state-of-the-art computer vision and machine learning algorithms. These algorithms can be used to detect and recognize faces, identify objects, classify human actions in videos, track camera movements, track moving objects, extract 3D models of objects, produce 3D point clouds from stereo cameras, stitch images together to produce a high resolution image of an entire scene, find similar images from an image database, remove red eyes from images taken using flash, follow eye movements, recognize scenery and establish markers to overlay it with augmented reality, etc.

5.1 Module Description

5.1.1 Module 1:Preprocessing

RGB images were converted to gray images using the function $cv2.cvtColor$ and the flag $cv2.COLOR\_BGR2GRAY$.

5.1.2 Image Acquisition and Dataset Creation

A set of captured images are given as an input to the system. These consist of multiple images of each subject which forms the dataset to train the algorithm. Images of the same person are given the same ID. Various sample input images are provided to the system to check the accuracy of the predictions and make necessary changes if required.

5.1.3 Face Detection

First, a classifier is trained with a few sample views of a particular face, called positive examples, that are scaled to the same size, and negative examples - arbitrary images of the same size.
After a classifier is trained, it can be applied to a region of interest (of the same size as used during the training) in an input image. The image captured in the previous module is accepted as the input. The classifier outputs a 1 if the region is likely to show the object, and 0 otherwise. To

search for the object in the whole image one can move the search window across the image and check every location using the classifier. The classifier is designed so that it can be easily resized in order to be able to find the objects of interest at different sizes, which is more efficient than resizing the image itself. So, to find an object of an unknown size in the image the scan procedure should be done several times at different scales.

5.1.4 Face Recognition

A face recognition system is a computer application capable of identifying a person from a digital image.This can be accomplished by comparing selected facial features with a face database. Many factors influence the process of face recognition such as shape, size, pose, occlusion, and illumination. The system is expected to detect the faces from the image regardless of direction and lighting.

5.1.5 Web Interface

The web interface can be made use by the bank officials. The bank offiials can login in and view the alert log and monitor the activities happening inside the ATM kiosk through the live videofeed from the camera placed inside the ATM.

Chapter 6

Data Flow Diagram

6.1 Level 0 DFD

DFD Level 0 is also called a Context Diagram. Its a basic overview of the whole system or process being analyzed or modeled. Its designed to be an at-a-glance view,showing the system as a single high-level process,with its relationship to external entities. It should be easily understood by a wide audience, including stakeholders, business analysts, data analysts and developers.

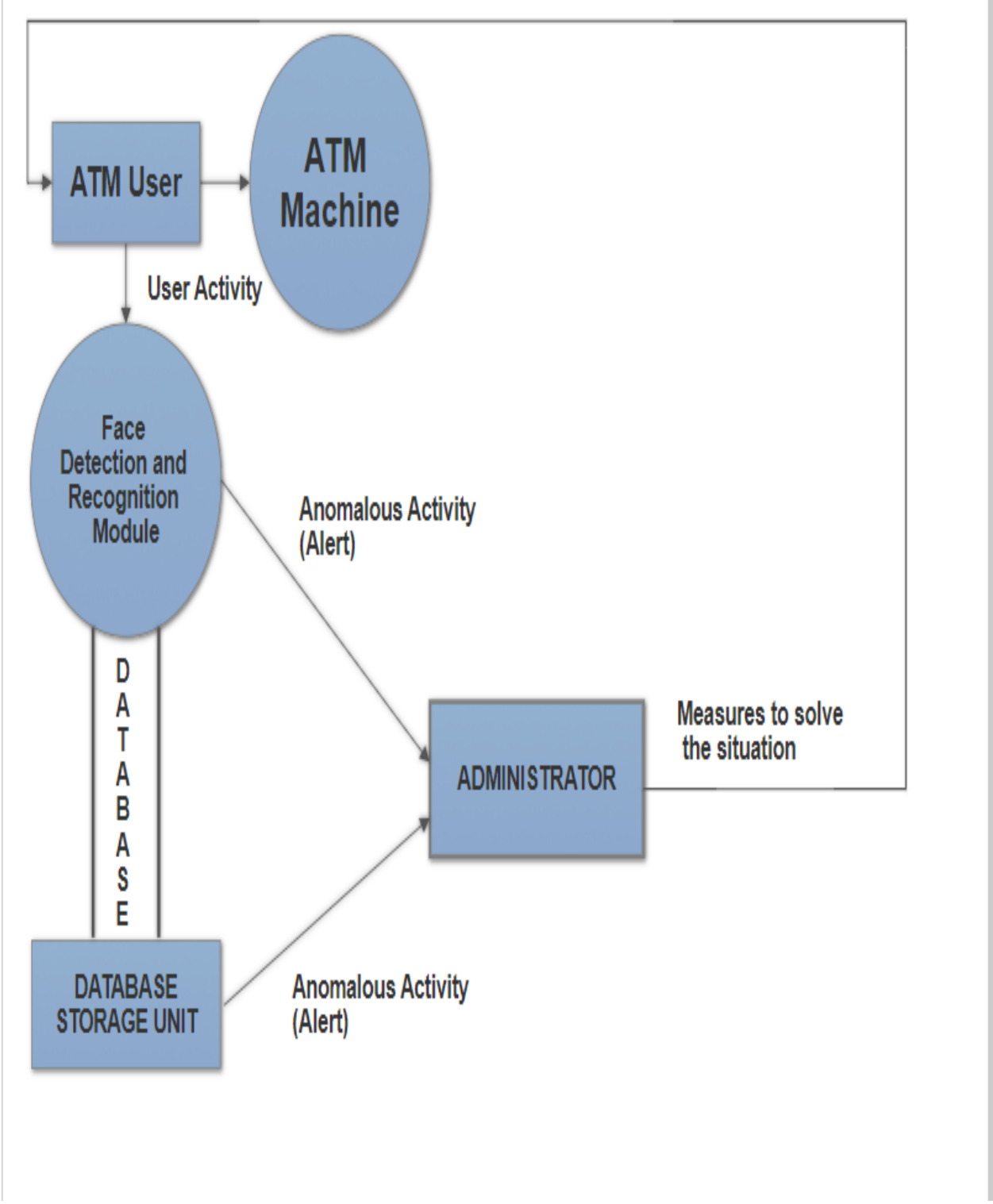


Figure 6.1: DFD Level 0

6.2 Level 1 DFD

DFD Level 1 provides a more detailed breakout pieces of the Context Level Diagram. You will highlight the main functions carried out by the system, as you break down the high-level process of the Context Diagram into its subprocess.Here we can see that, the uploaded videos from the video library fed is fed to the Low Level Feature Extraction unit.Sequentially the data extracted is fed to the concept detector and then subject to concept adjustment. Finally it is indexed using the technique of inverted indexing.

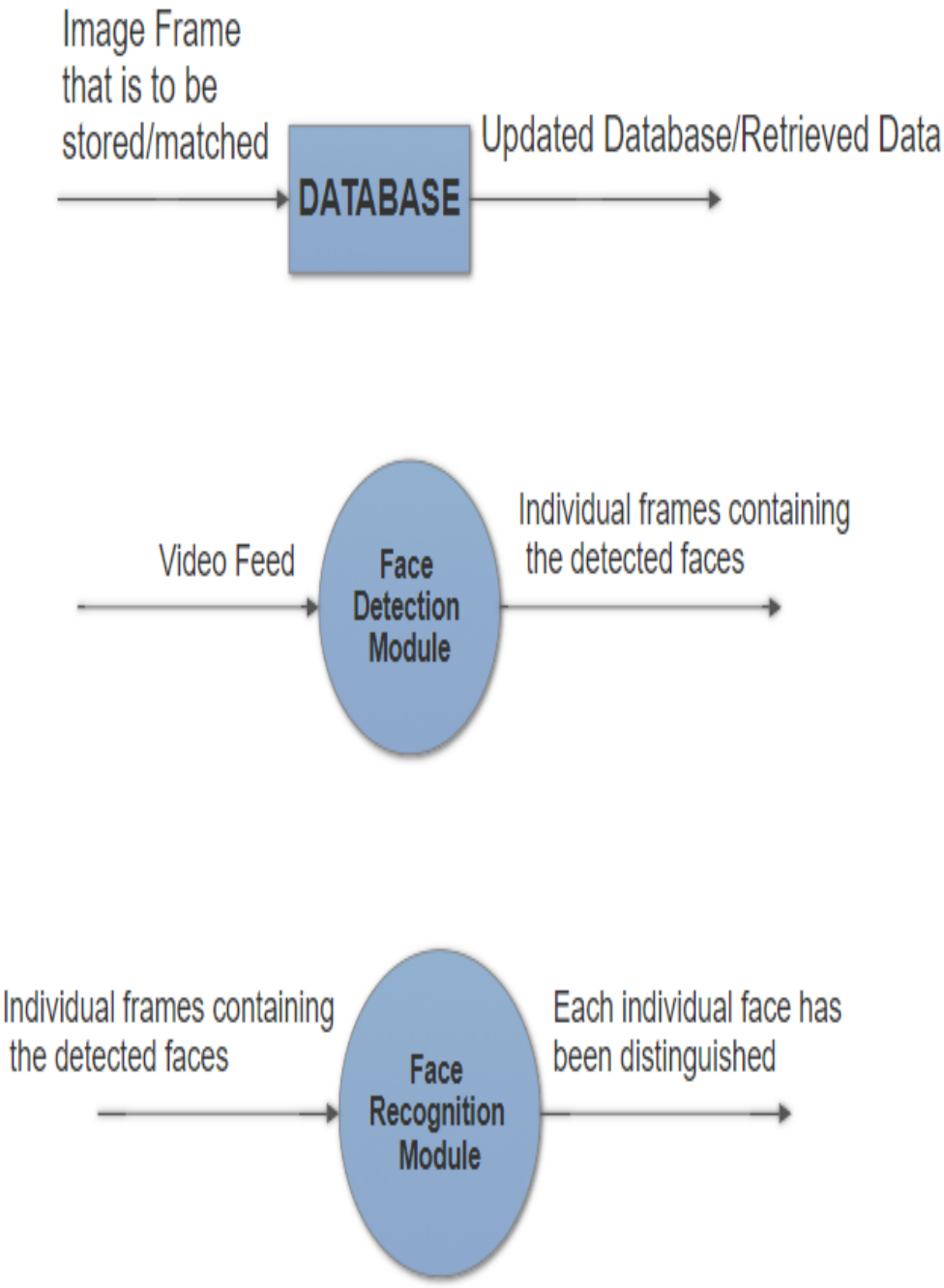


Figure 6.2: DFD Level 2 (Face Detection Module)

Chapter 7

Implementation

7.1 Algorithms

This section explains the pseudocodes of the algorithms that will be used in the implementation of the project.

7.1.1 Algorithm 1

1. Person enters the kiosk.
2. Check for the following conditions
. a.If the person is wearing a mask.
. b.If there are more than three people inside the kiosk.
. c.If the same person enters the kiosk more than thrice in an hour.
3. If any of the following conditions becomes true issue an alert.

7.1.2 Algorithm 2 : Face Detection

1. Take as input a frame from the video feed.
2. Perform Upper Body Detection.
3. Perform Eye Detection.
4. If any of the above steps results in an error issue an alert.

7.1.3 Algorithm 3 : Eye Detection

1. Eyes are detected based on the hypothesis that they are darker than other part of the face.
2. The alignment of the two major axis, so that the two eye regions belong to the same line.
3. Perform Iris recognition.
. a. A binary edge map based on gradient based is constructed from the intensities of the pixels in an iris image.
. b. the iris inner and outer borders are detected using Hough transform
4. If conditions not satisfied return error.

7.1.4 Algorithm 4 : Face Recognition

1. After face detection, using the pixel positions, convert the image into a feature matrix.
2. Check if the same feature matrix already exists in the database.
3. If it does increase the count for the matrix by 1.
2. If it doesn't already exist, add it to the database with count 1.

7.2 Development Tools

Git is a version control system (VCS) for tracking changes in computer files and coordinating work on those files among multiple people. It is primarily used for software development, but it can be used to keep track of changes in any file. As a distributed revision control system it is aimed at speed, data integrity and support for distributed, non-linear workflows. Git was created by Linus Torvalds in 2005 for development of the Linux kernel, with other kernel developers contributing to its initial development. Its current maintainer since 2005 is Junio Hamano. As with most other distributed version control systems, and unlike most clientserver systems, every Git directory on every computer is a full-fledged repository with complete history and full version tracking abilities, independent of network access or a central server. Like the Linux kernel, Git is free software distributed under the terms of the GNU General Public License version 2. Usage of Git in this project helped in keeping track of code and issues. It also helped integrating the work during each development phase. Without Git the project would be messy and combining the work of all contributors would have been more time-consuming than necessary.

Chapter 8

Testing

8.1 Testing Methodologies

Software Testing Methodology is defined as strategies and testing types used to certify that the Application Under Test meets user expectations. Test Methodologies include functional and non-functional testing to validate the Application Under Test. Each testing methodology has a defined test objective, test strategy and deliverables. We performed the following testing: Unit testing, Integration testing, System testing, Performance testing.

8.2 Unit Testing

Unit testing is the first level of testing and is often performed by the developers themselves. It is the process of ensuring individual components of a piece of software at the code level are functional and work as they were designed to. Developers in a test-driven environment will typically write and run the tests prior to the software or feature being passed over to the test team. Unit testing can be conducted manually, but automating the process will speed up delivery cycles and expand test coverage. Unit testing will also make debugging easier because finding issues earlier means they take less time to fix than if they were discovered later in the testing process.

The primary goal of unit testing is to take the smallest piece of testable software in the application, isolated from the remainder of the code, and whether it behaves exactly as we expect. Each unit is tested separately before integrating them into modules to test the interfaces between modules. Unit Testing is a software verification and validation method where programmer gains confidence that individual units of source code are error free for future use. We did unit testing on the following modules:-

- Eye Detection : Test on an image to detect eyes based on Haar classifier algorithm.
- Mouth Detection : Test on an image to detect mouth based on Haar classifier algorithm.
- Face Detection : Test on an image to detect faces based on Haar classifier algorithm.
- Face Recognition : Test on the image to recognize the faces by comparing them with the faces in the database.
- Database : Tested a python program that creates a MySQL databse and manipulates it.

- Web Interface : Created a web interface to view and update attendance.

8.3 Integration Testing

After each unit is thoroughly tested, it is integrated with other units to create modules or components that are designed to perform specific tasks or activities. These are then tested as group through integration testing to ensure whole segments of an application behave as expected (i.e, the interactions between units are seamless). These tests are often framed by user scenarios, such as logging into an application or opening files. Integrated tests can be conducted by either developers or independent testers and are usually comprised of a combination of automated functional and manual tests.

This testing strategy combines all the modules involved in the system. After the independant modules are tested, dependant modules that use the independant modules are tested. This sequence of testing layers of dependant modules continues until the entire system is constructed. The modules of our project were added step by step so that addition of a module does not affect the performance of another.

We integrated our modules one by one and tested the partially integrated system.;

8.4 System Testing

System testing is a black box testing method used to evaluate the completed and integrated system, as a whole, to ensure it meets specified requirements. The functionality of the software is tested from end-to-end and is typically conducted by a separate testing team than the development team before the product is pushed into production.

All modules were integrated at the end of integration testing and the entire system was tested by taking an image of a group of students and checking if the faces are recognized and the attendance is updated.

This testing strategy combines all the modules involved in the system. After the independant modules are tested, dependant modules that use the independant modules are tested. In our project we have combined all the functionalities and has been tested. The desired results were obtained.

Chapter 9

Graphical User Interface

9.1 GUI Overview

The main application consists of a web interface which uses the django framework that allows the bank officials to login, view alert issue log and monitor the live videofeed from the camera placed inside the ATM kiosk.

The web interface ensures that the bank officials can access information regarding the alerts issued at all times.

9.2 Main GUI Components

9.2.1 Login

This component deals with the authentication of the users. Bank officials may login with their credentials which directs them to the dashboard.

The dashboard enables the bank officials to view the alert log and access the live video feed from the camera placed inside the ATM.

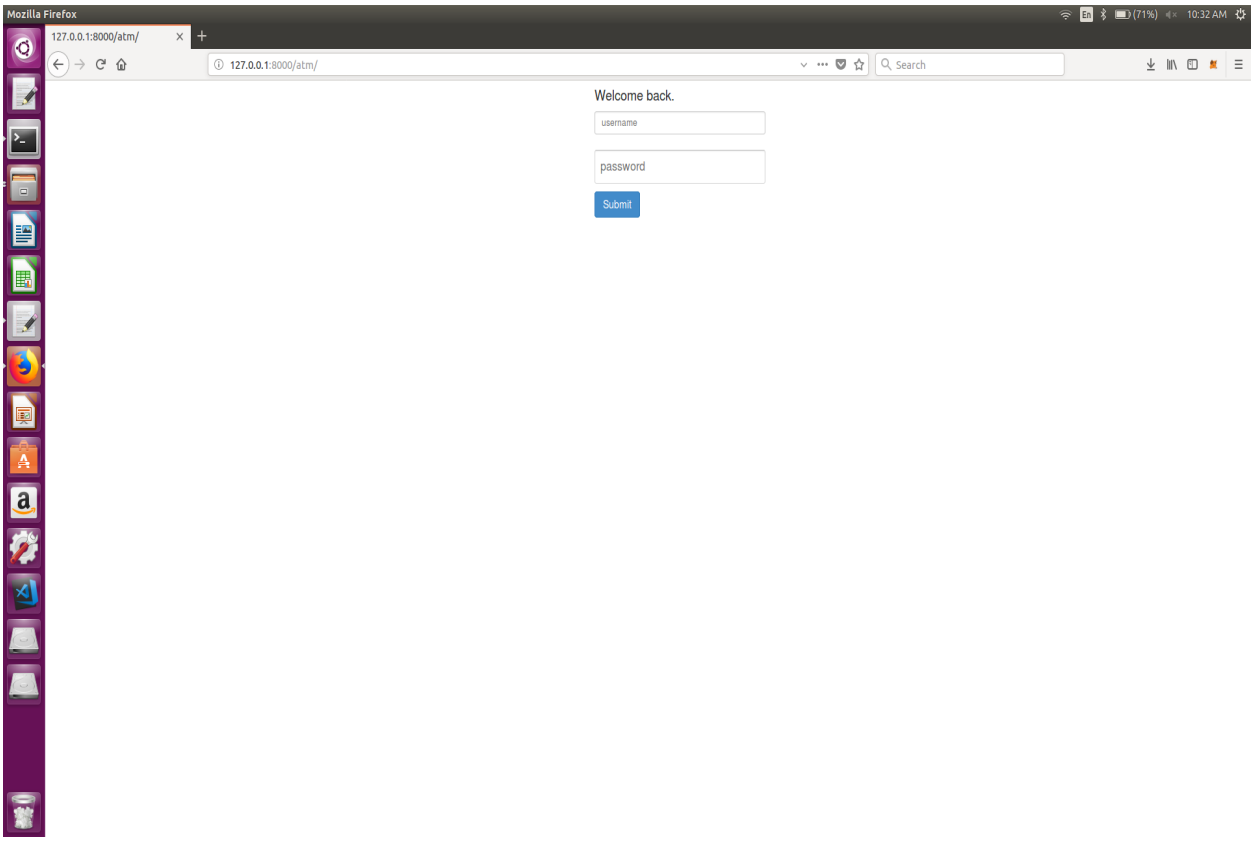


Figure 9.1: Login

9.2.2 Home Page

After logging in the bank officials are redirected to the home page. The home page contains two buttons. Using these buttons the officials can go to the page containing the alert log and another page containing the video feed.

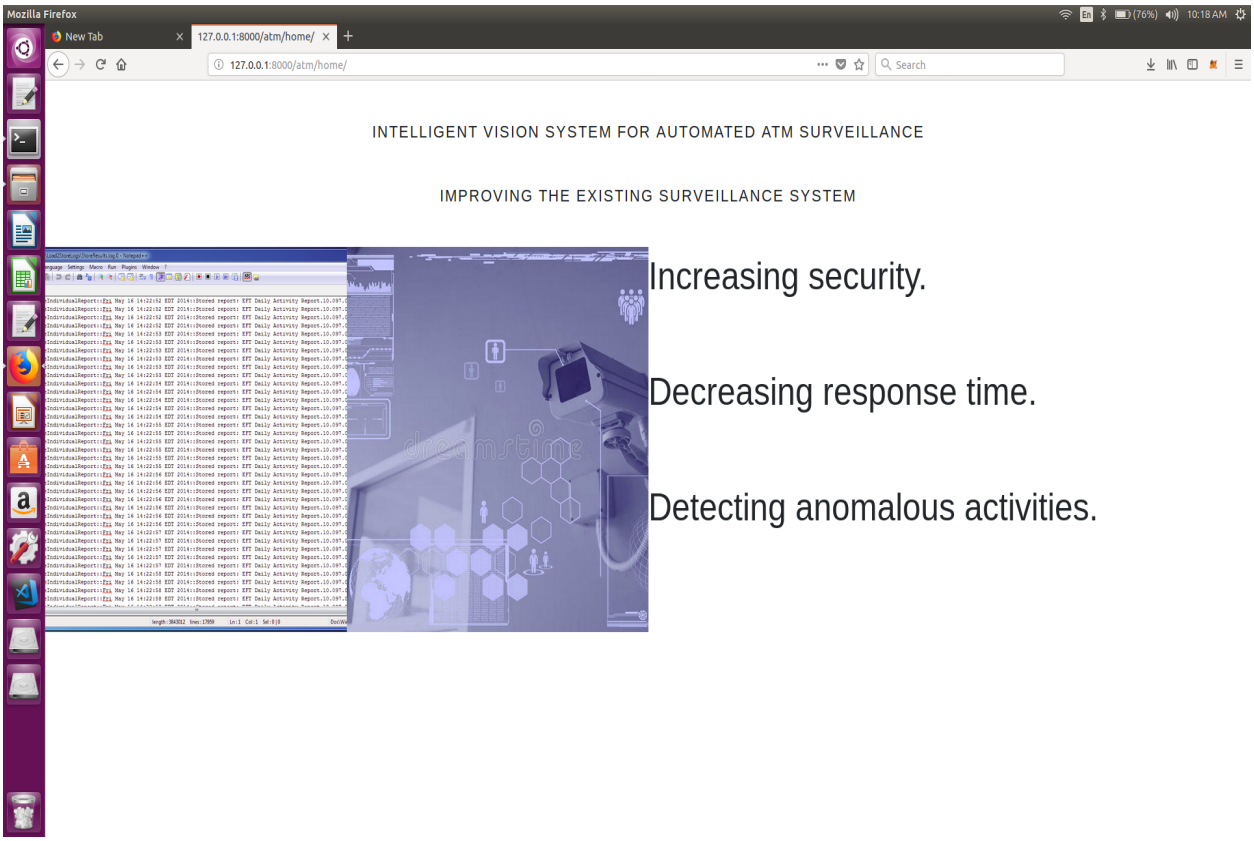


Figure 9.2: Home page

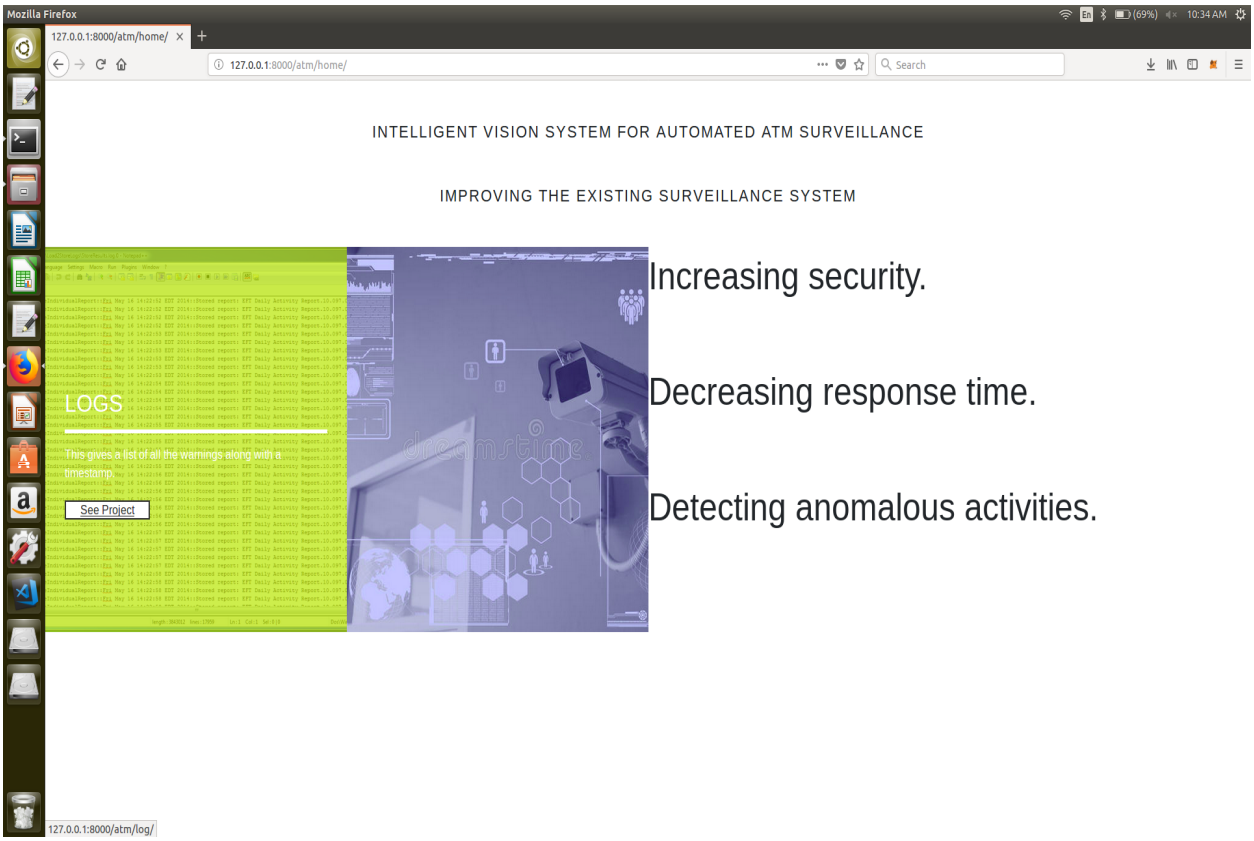


Figure 9.3: Home page with Log Button selected

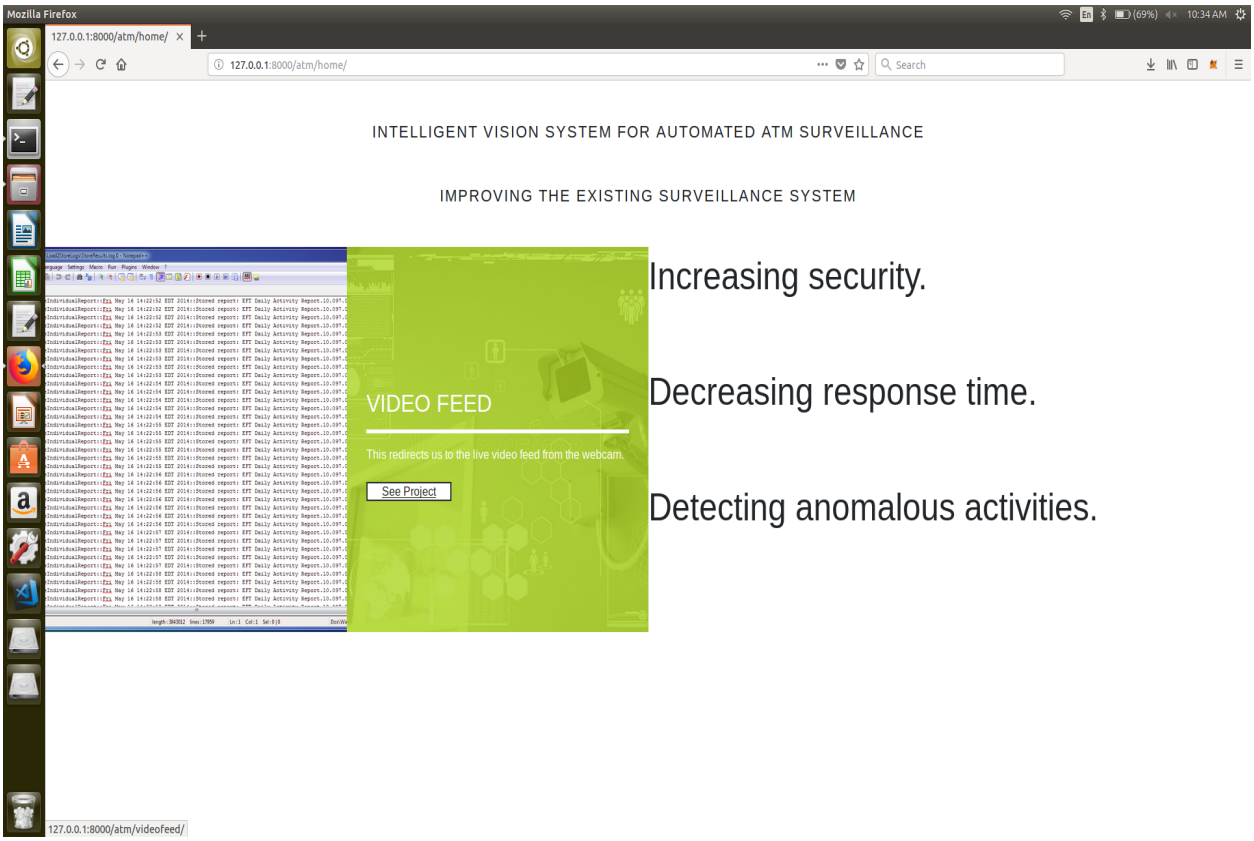
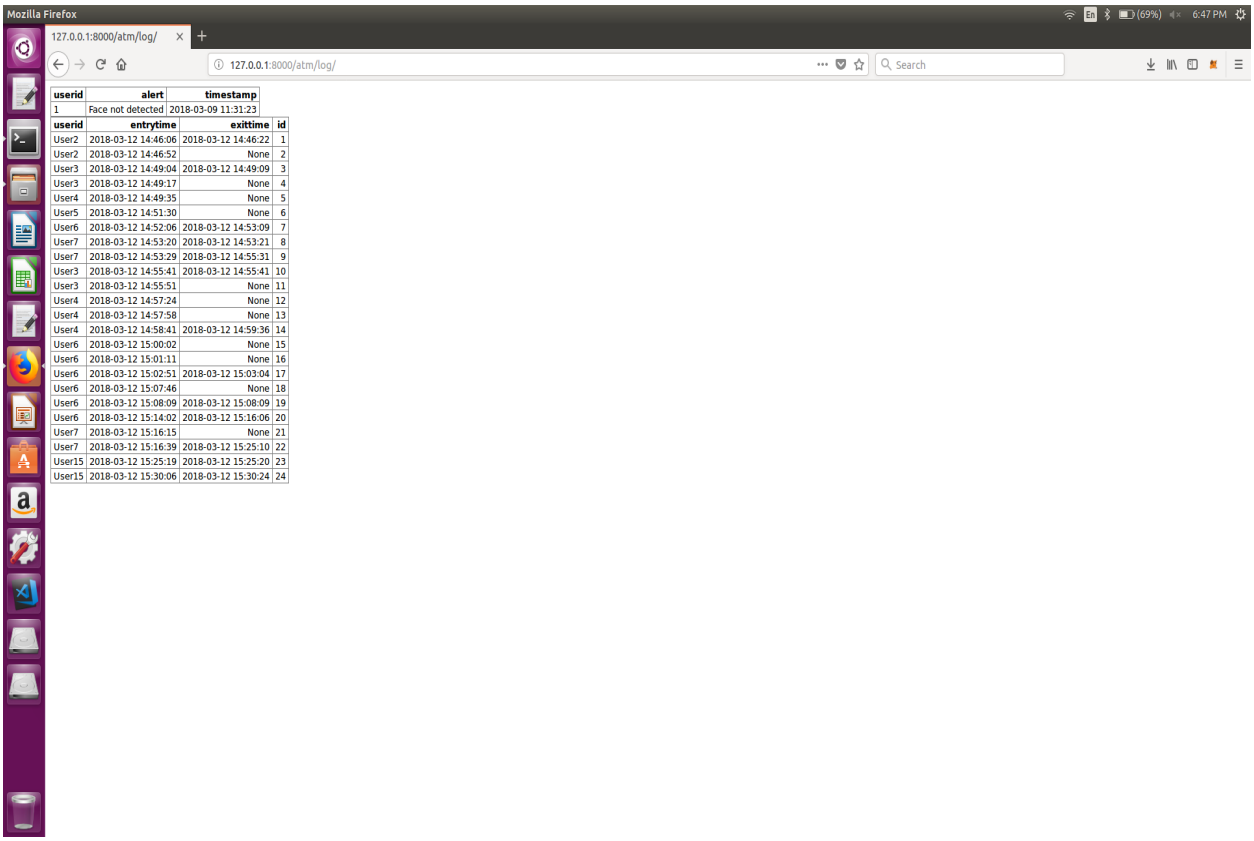


Figure 9.4: Home page with Video feed Button selected

9.2.3 Alert Issue Log Page

This page contains data on all the alerts issued. It displays all the alert issued along with the alert type and the time at which the alert was issued. It also contains a navigation bar. We can move to the page displaying the video feed and to the home page using the navigation bar.



userid	alert	timestamp
1	Face not detected	2018-03-09 11:31:23

userid	entrytime	exittime	id
User2	2018-03-12 14:46:06	2018-03-12 14:46:22	1
User2	2018-03-12 14:46:52	None	2
User3	2018-03-12 14:49:04	2018-03-12 14:49:09	3
User3	2018-03-12 14:49:17	None	4
User4	2018-03-12 14:49:35	None	5
User5	2018-03-12 14:51:30	None	6
User6	2018-03-12 14:52:06	2018-03-12 14:53:09	7
User7	2018-03-12 14:53:20	2018-03-12 14:53:21	8
User7	2018-03-12 14:53:29	2018-03-12 14:55:31	9
User3	2018-03-12 14:55:41	2018-03-12 14:55:41	10
User3	2018-03-12 14:55:51	None	11
User4	2018-03-12 14:57:24	None	12
User4	2018-03-12 14:57:58	None	13
User4	2018-03-12 14:58:41	2018-03-12 14:59:36	14
User6	2018-03-12 15:00:02	None	15
User6	2018-03-12 15:01:11	None	16
User6	2018-03-12 15:02:51	2018-03-12 15:03:04	17
User6	2018-03-12 15:07:46	None	18
User6	2018-03-12 15:08:09	2018-03-12 15:08:09	19
User6	2018-03-12 15:14:02	2018-03-12 15:16:06	20
User7	2018-03-12 15:16:15	None	21
User7	2018-03-12 15:16:39	2018-03-12 15:25:10	22
User15	2018-03-12 15:25:19	2018-03-12 15:25:20	23
User15	2018-03-12 15:30:06	2018-03-12 15:30:24	24

Figure 9.5: Alert Issue Log Page

9.2.4 Video Feed Page

This page contains a window which displays the live video feed from the camera placed inside the ATM kiosk. It also contains a navigation bar. We can move to the page displaying the alert issue log and to the home page using the navigation bar.

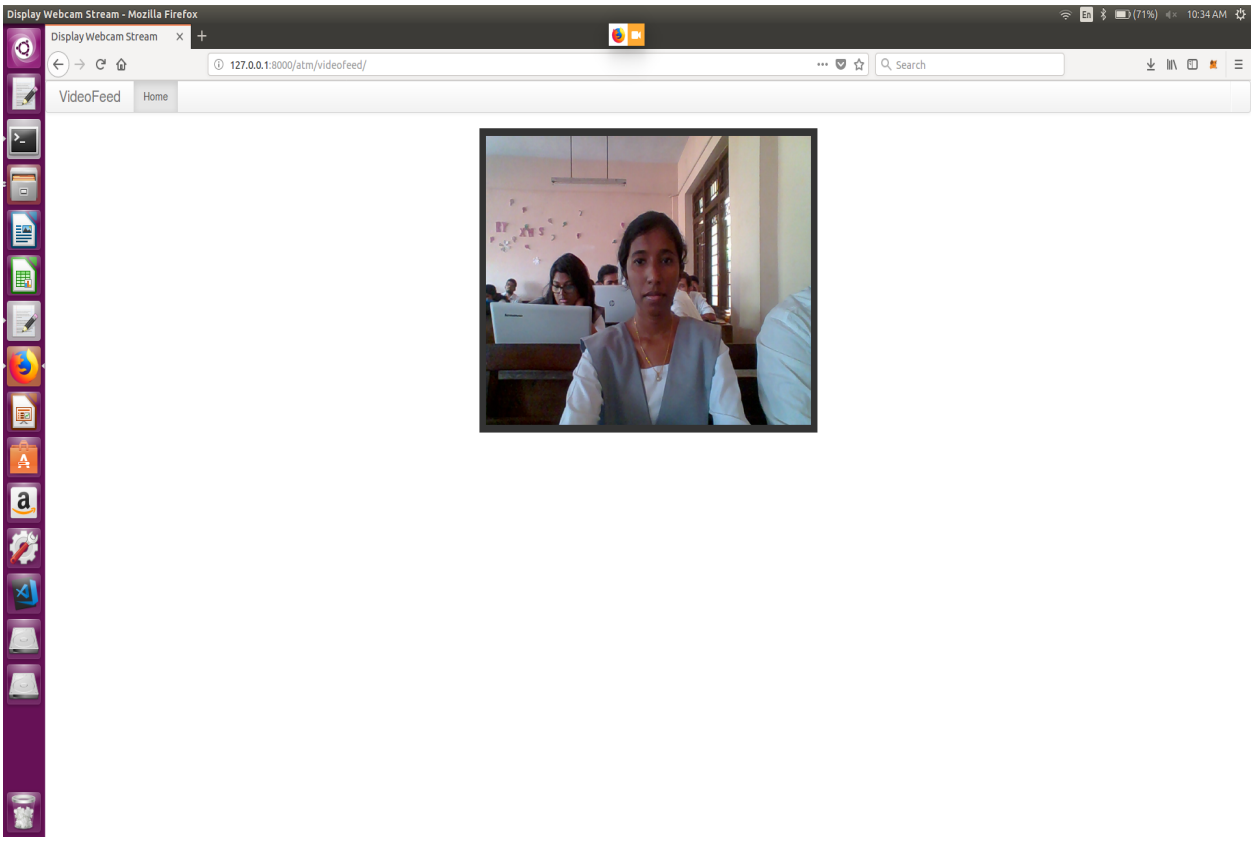


Figure 9.6: Video Feed Page

Chapter 10

Results

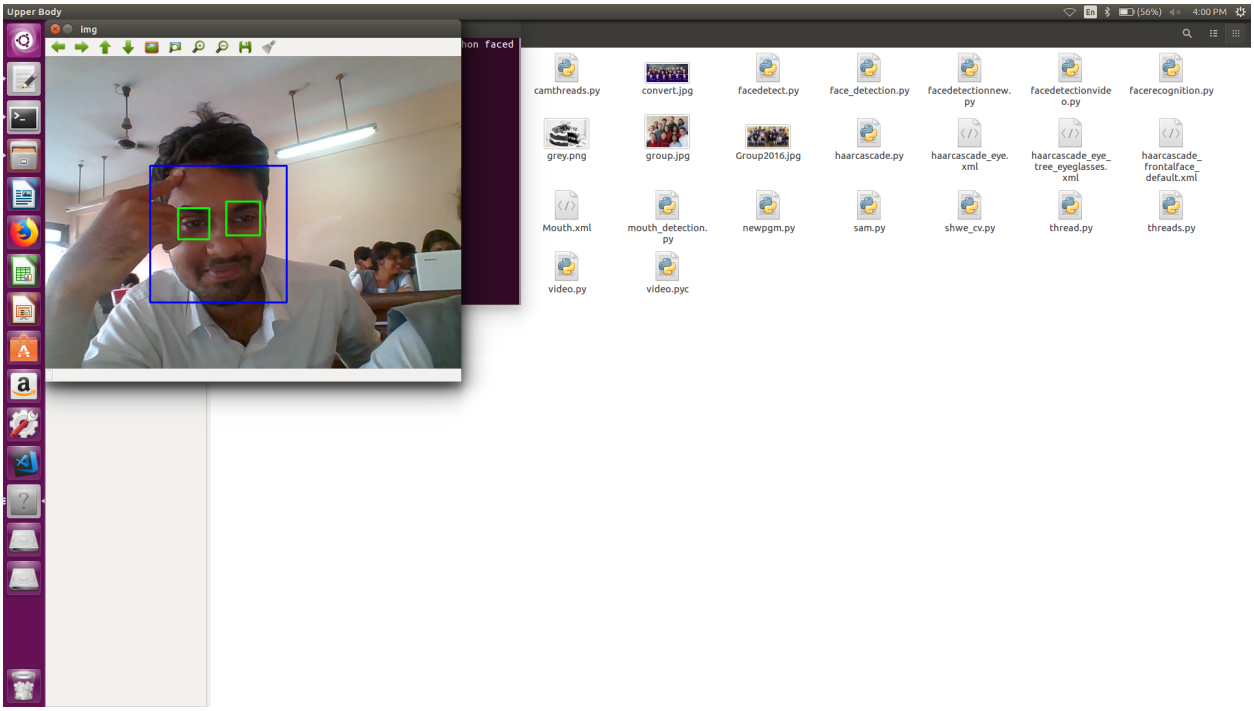


Figure 10.1: Face Detection Module

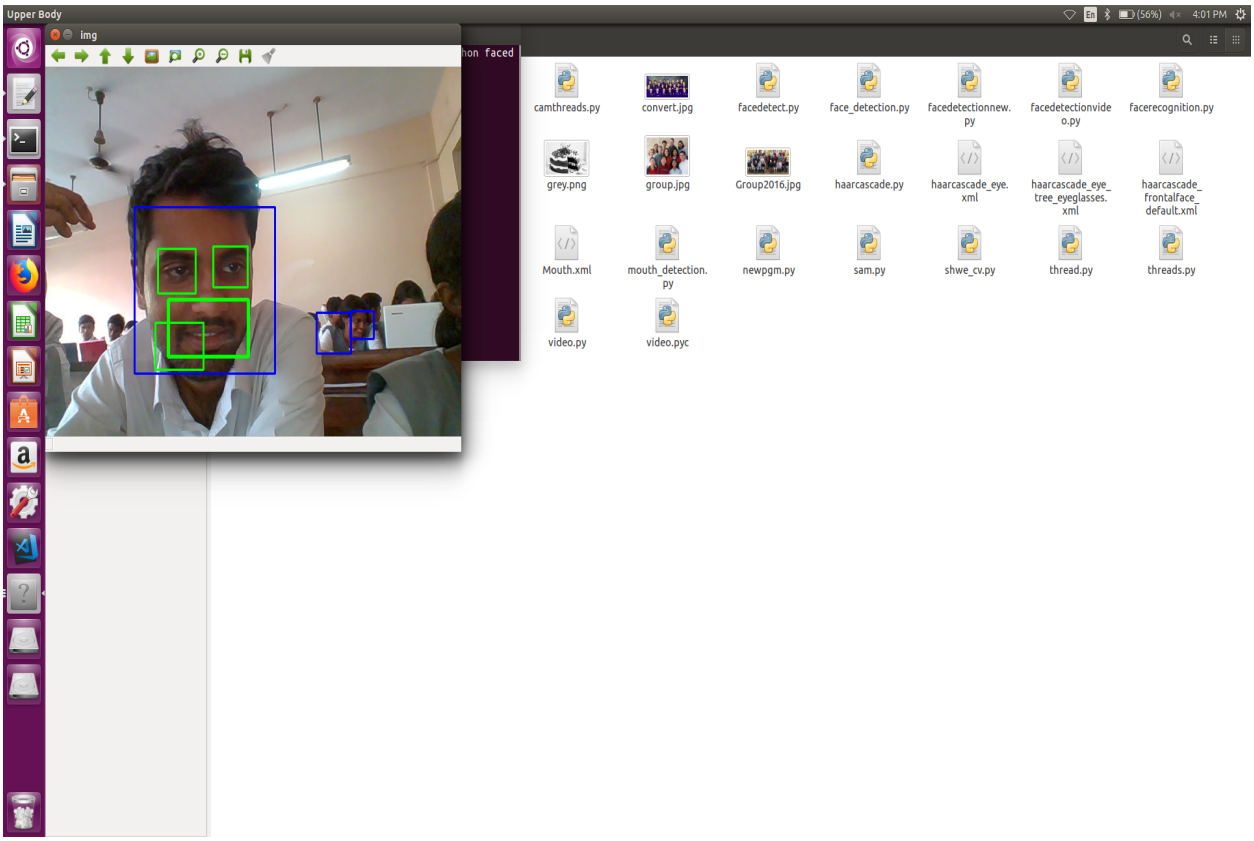


Figure 10.2: Face Detection Module

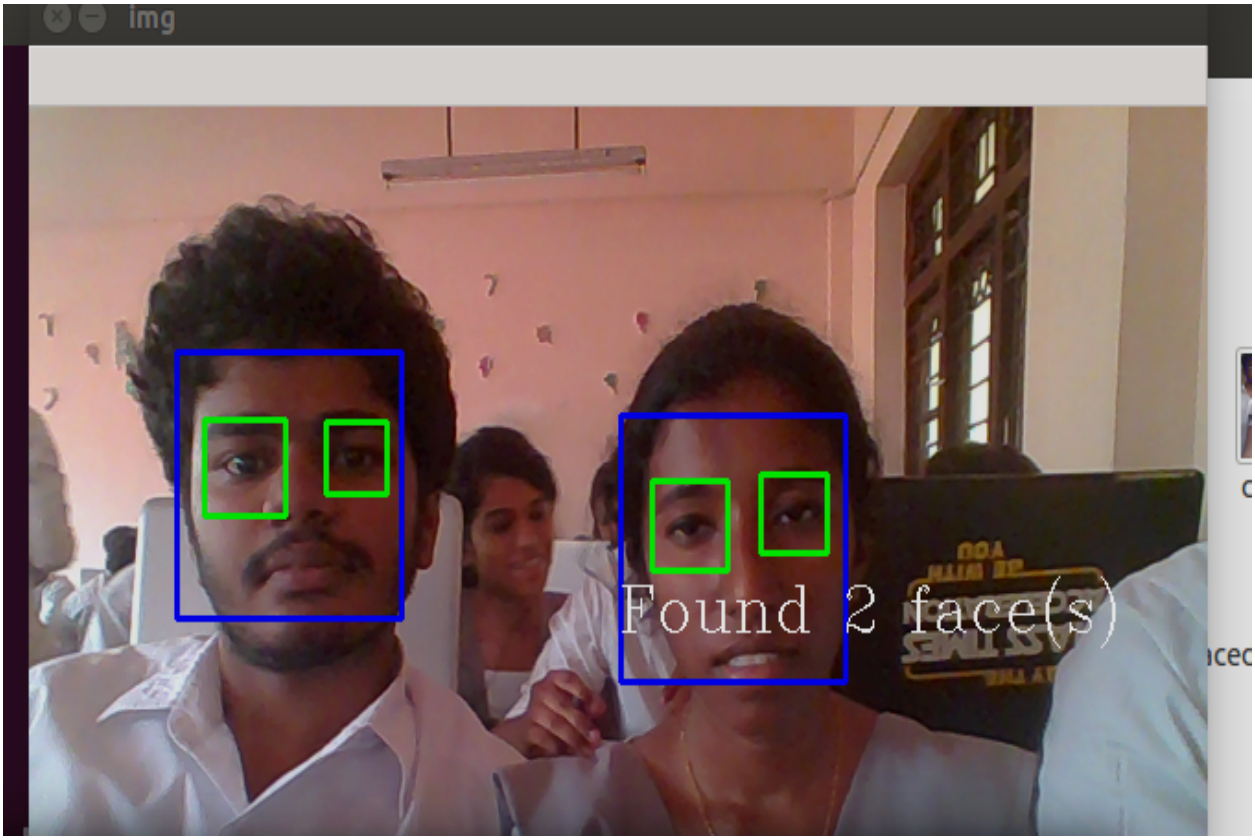


Figure 10.3: FaceDetection for more than one face

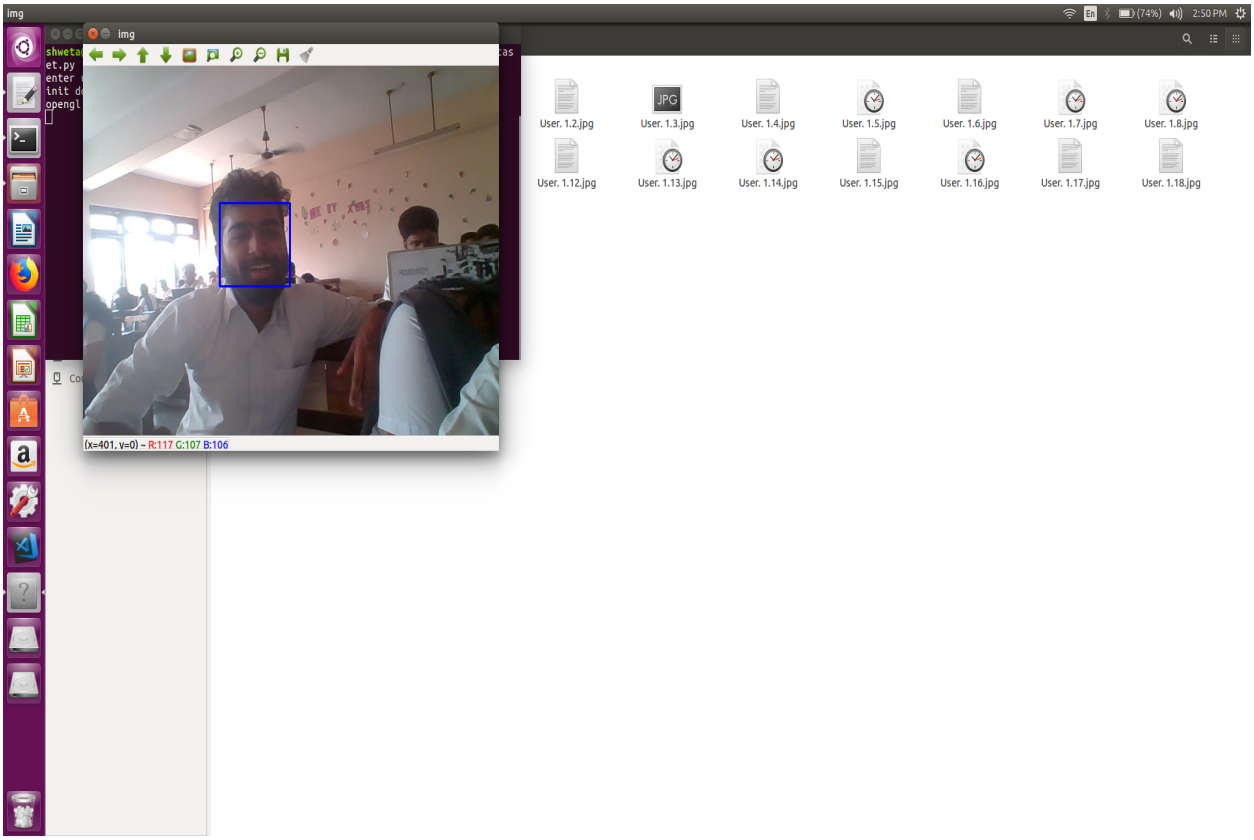


Figure 10.4: Facedetection for dataset creation

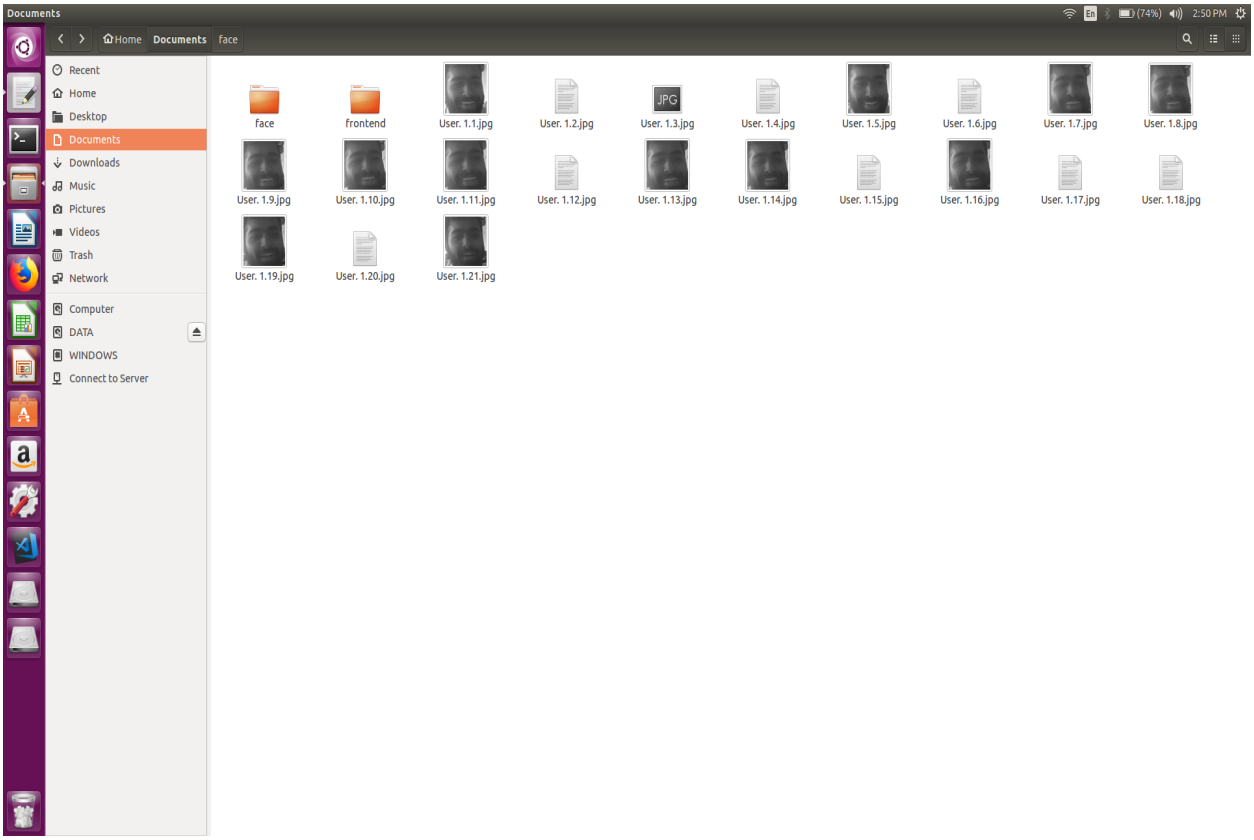


Figure 10.5: Dataset Creation

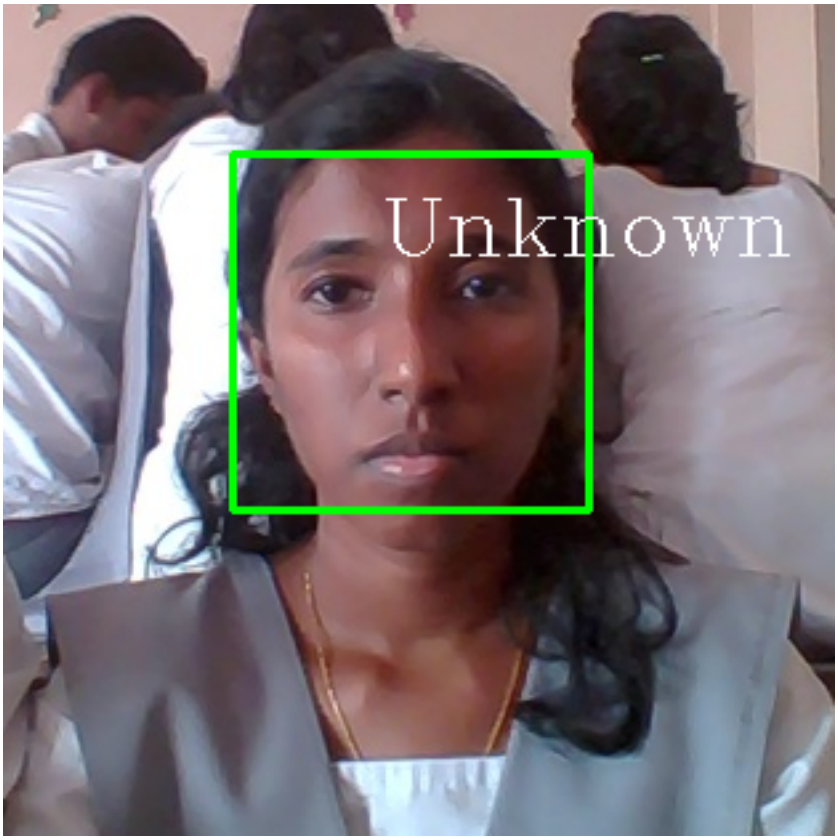


Figure 10.6: Face Recognition: First time

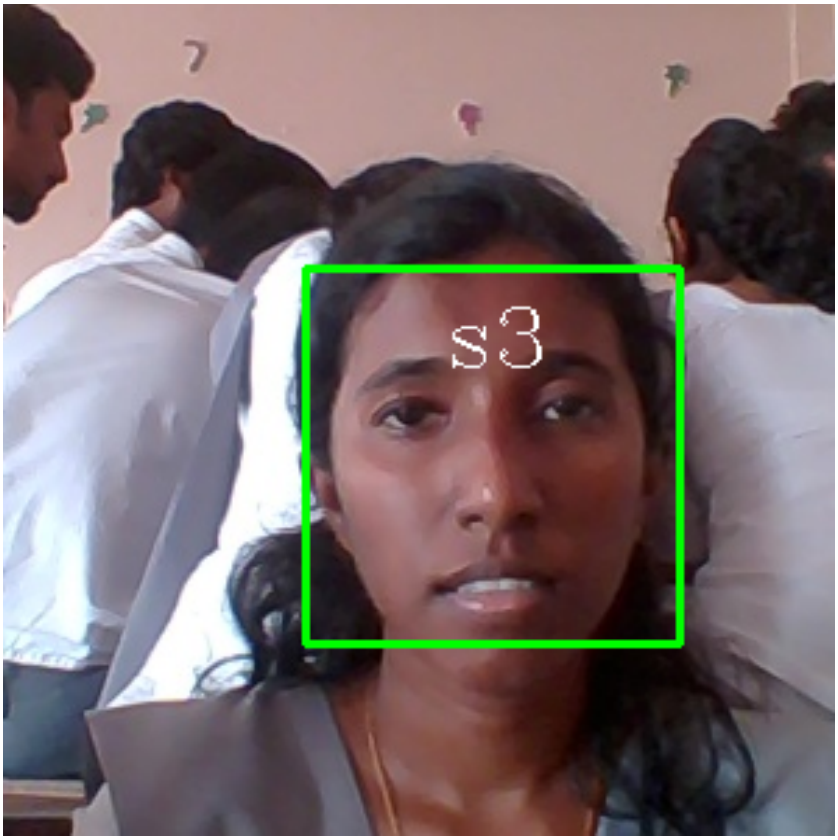


Figure 10.7: Face Recognition: Second time

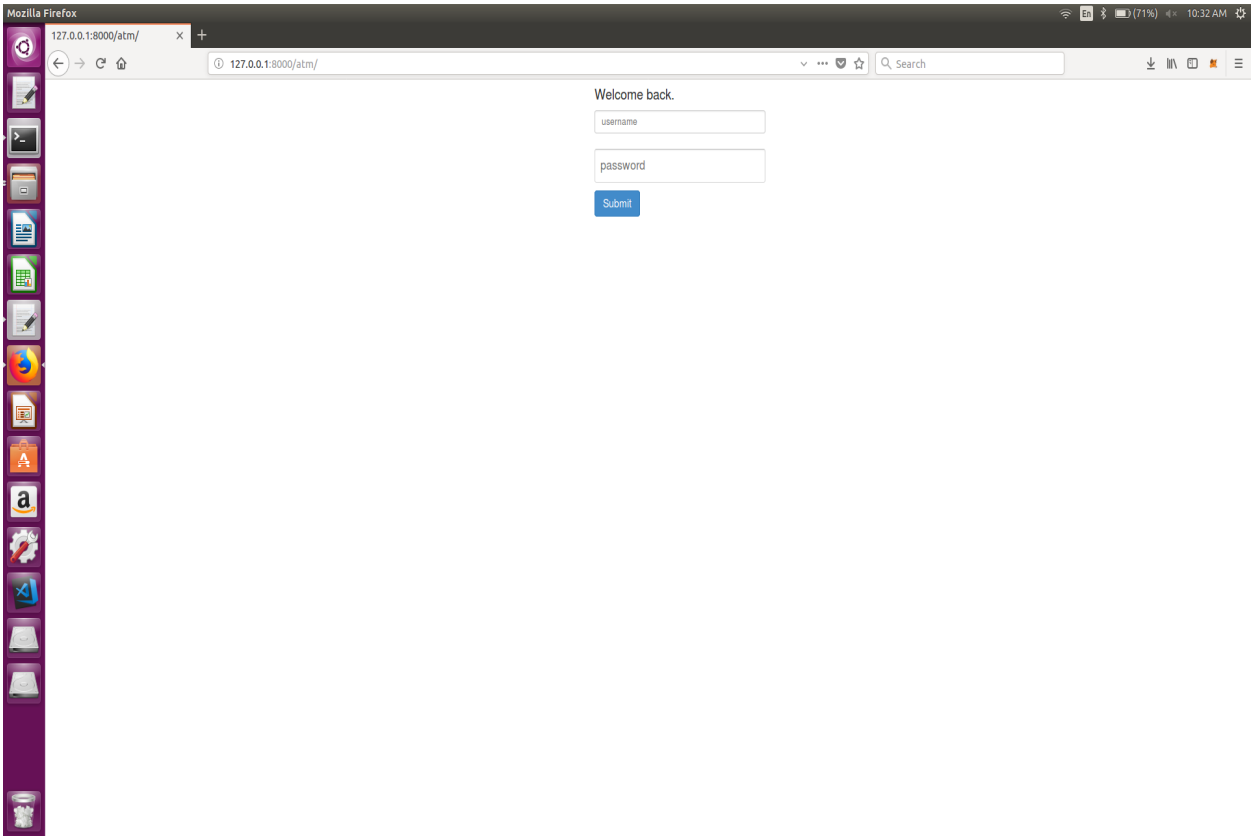


Figure 10.8: Web Interface - Log in Page

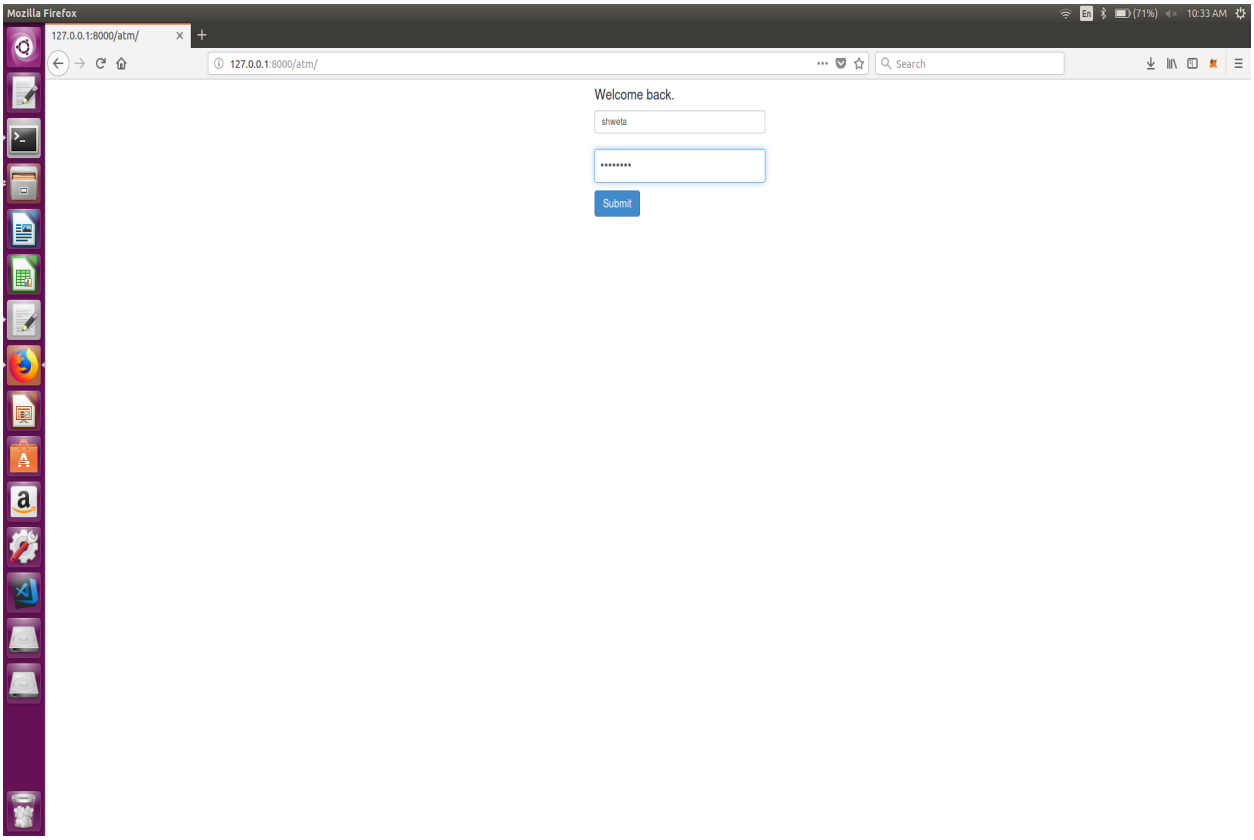


Figure 10.9: Web Interface - Log in page with User Credentials

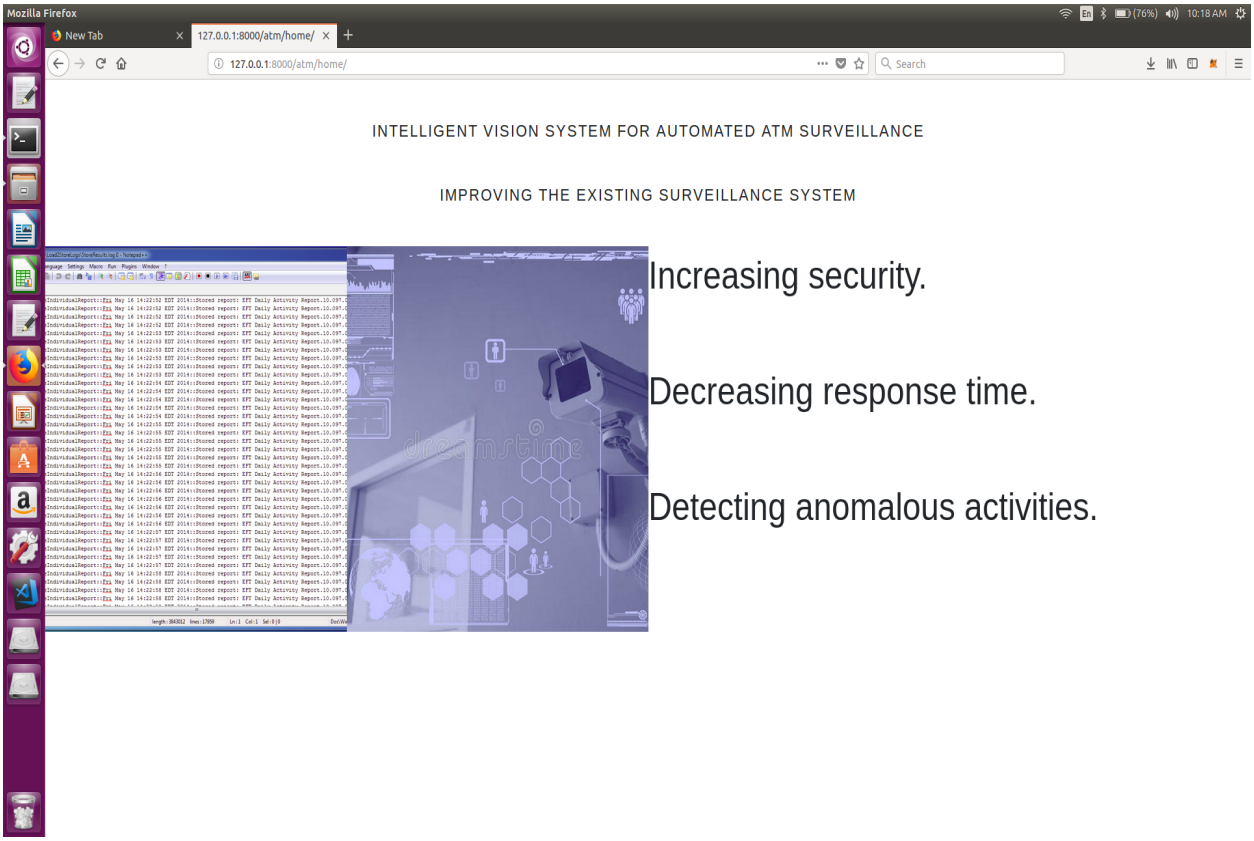


Figure 10.10: Web Interface - Home Page

,

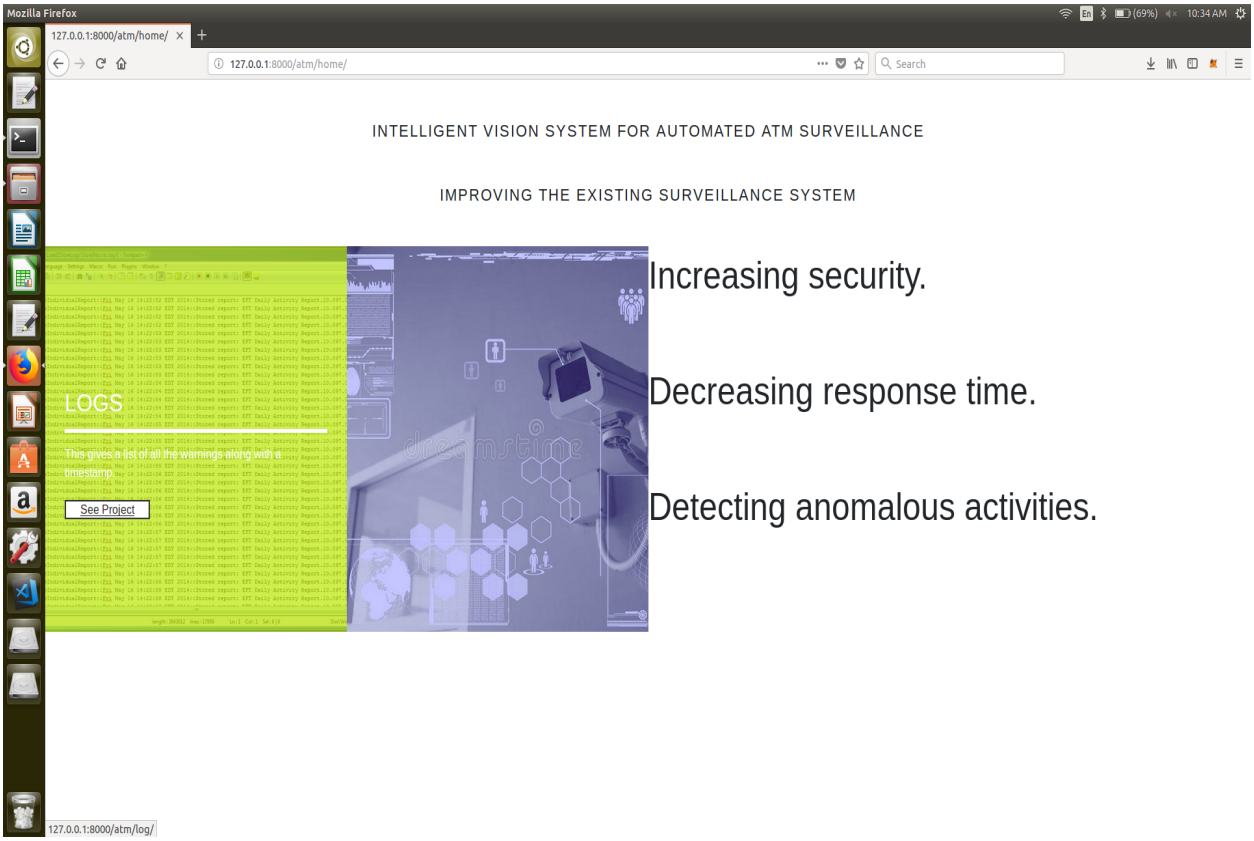


Figure 10.11: Web Interface - Home Page with Log Button

,

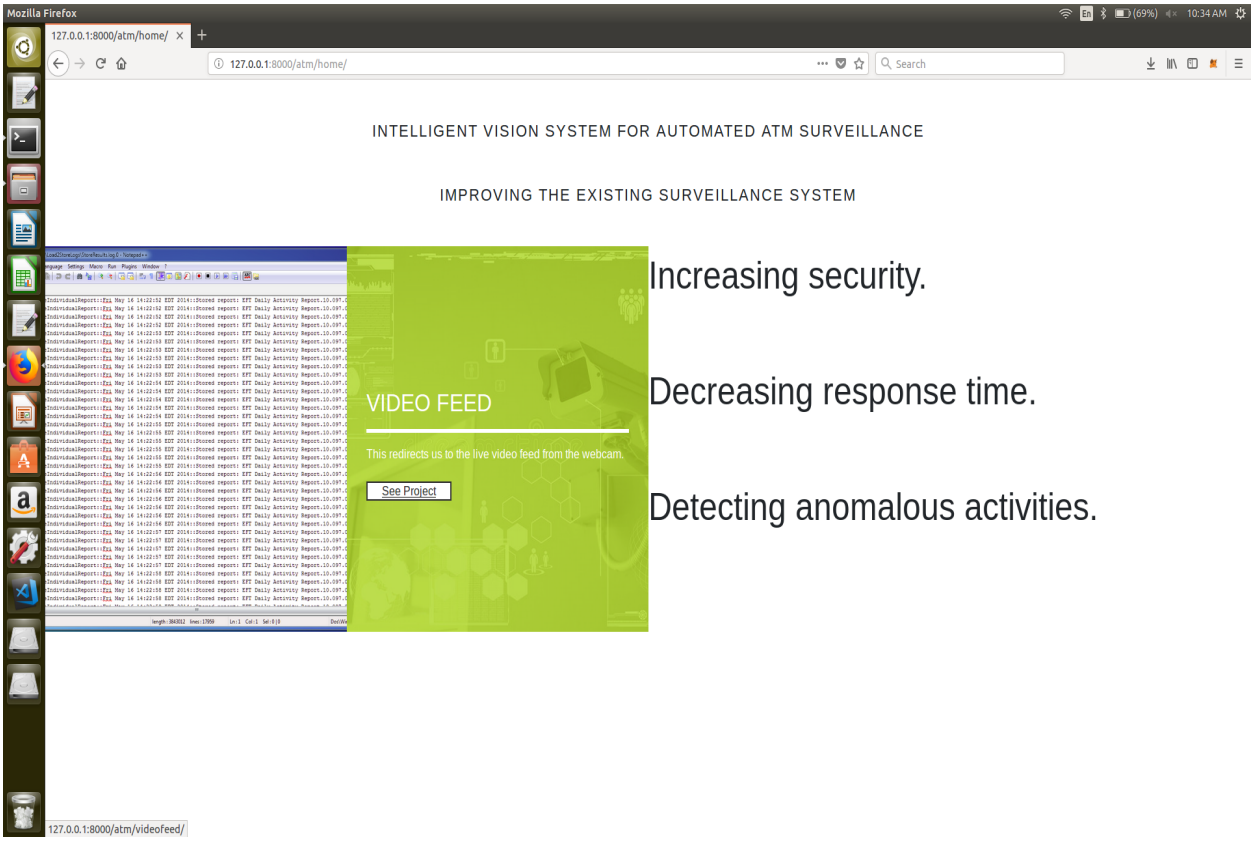
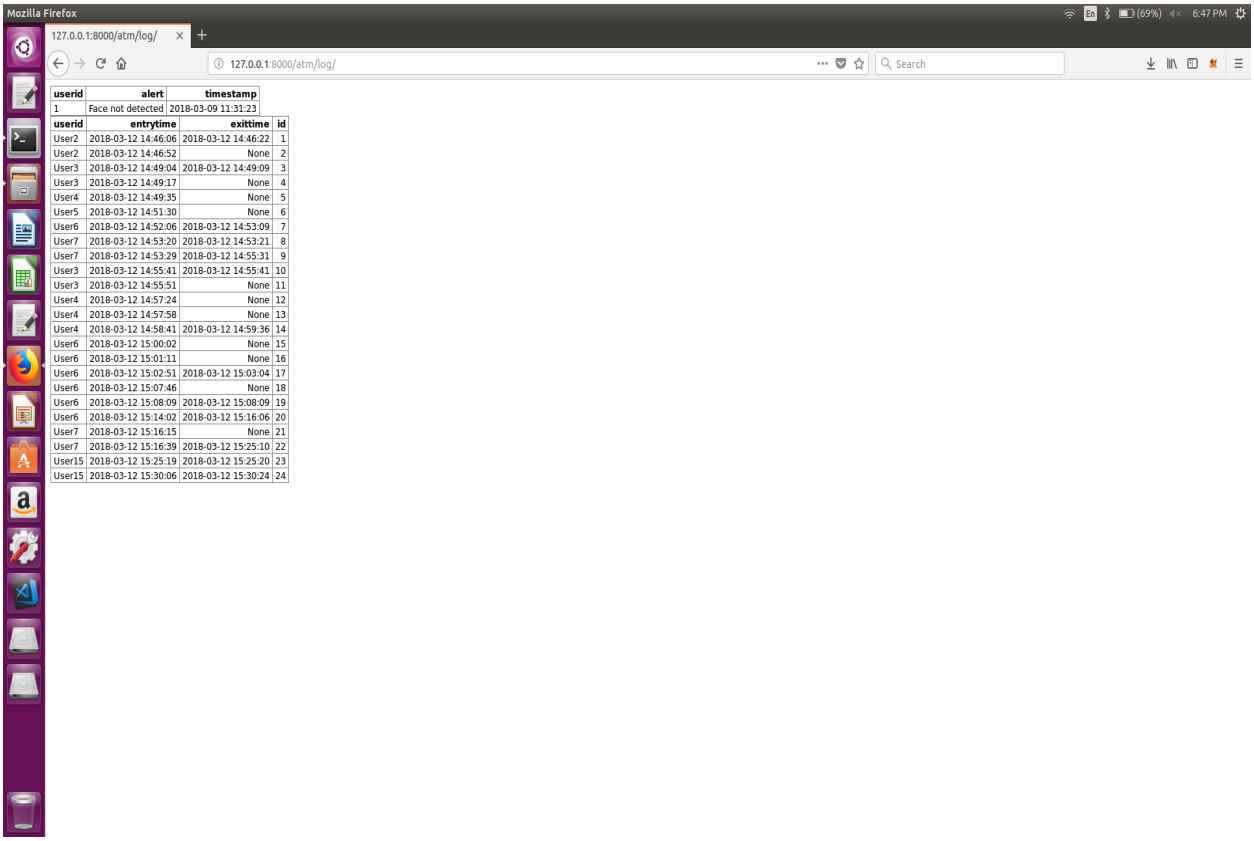


Figure 10.12: Web Interface - Home Page with Video Feed Button

,



userid	alert	timestamp
1	Face not detected	2018-03-09 11:31:23

userid	entrytime	exittime	id
User2	2018-03-12 14:46:06	2018-03-12 14:46:22	1
User2	2018-03-12 14:46:52	None	2
User3	2018-03-12 14:49:04	2018-03-12 14:49:09	3
User3	2018-03-12 14:49:17	None	4
User4	2018-03-12 14:49:35	None	5
User5	2018-03-12 14:51:30	None	6
User6	2018-03-12 14:52:06	2018-03-12 14:53:09	7
User7	2018-03-12 14:53:20	2018-03-12 14:53:21	8
User7	2018-03-12 14:53:29	2018-03-12 14:55:31	9
User3	2018-03-12 14:55:41	2018-03-12 14:55:41	10
User3	2018-03-12 14:55:51	None	11
User4	2018-03-12 14:57:24	None	12
User4	2018-03-12 14:57:58	None	13
User4	2018-03-12 14:58:41	2018-03-12 14:59:36	14
User6	2018-03-12 15:00:02	None	15
User6	2018-03-12 15:01:11	None	16
User6	2018-03-12 15:02:51	2018-03-12 15:03:04	17
User6	2018-03-12 15:07:46	None	18
User6	2018-03-12 15:08:09	2018-03-12 15:08:09	19
User6	2018-03-12 15:14:02	2018-03-12 15:16:06	20
User7	2018-03-12 15:16:15	None	21
User7	2018-03-12 15:16:39	2018-03-12 15:25:10	22
User15	2018-03-12 15:25:19	2018-03-12 15:25:20	23
User15	2018-03-12 15:30:06	2018-03-12 15:30:24	24

Figure 10.13: Web Interface - Alert Issue Log Page

,

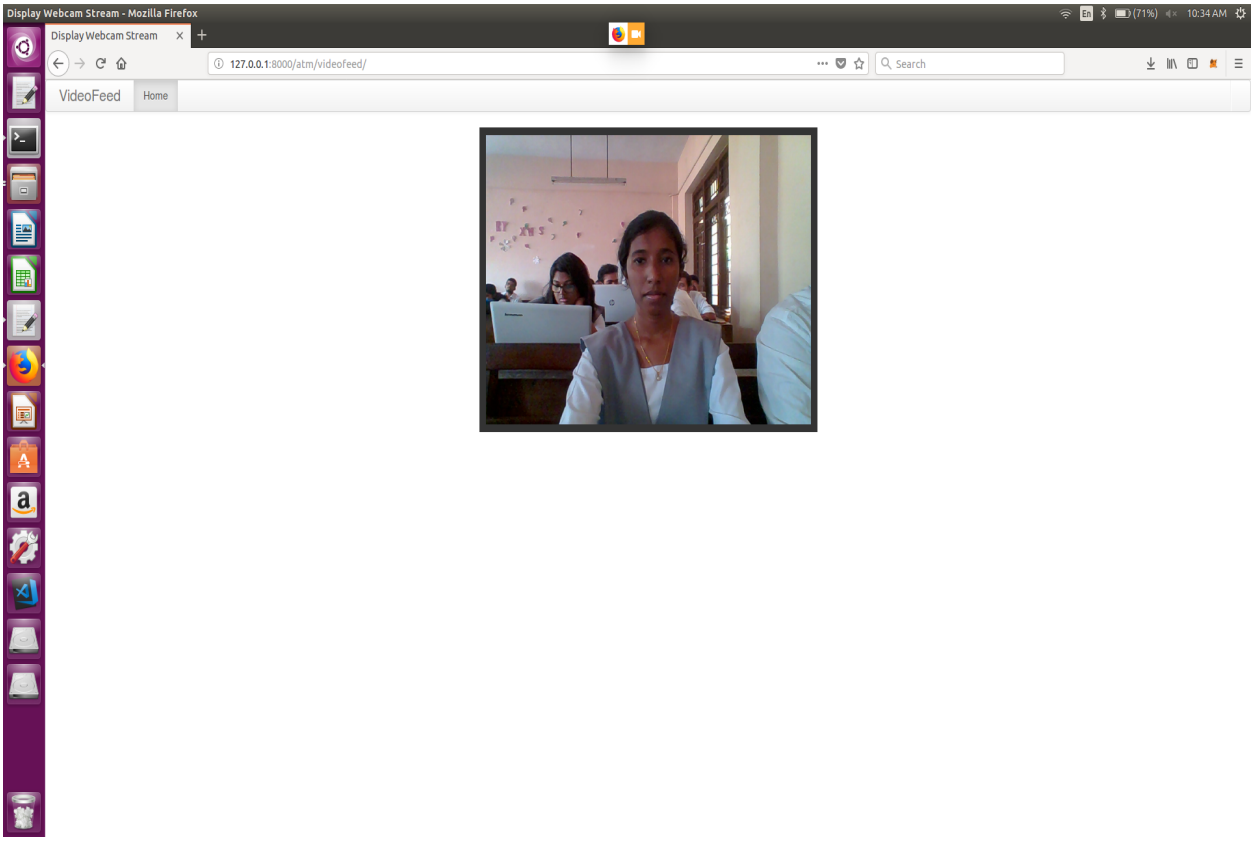


Figure 10.14: Web Interface - Video feed Page

,

Chapter 11

Conclusion

A fully functional Intelligent Vision System for monitoring Security and Surveillance of ATM is developed using OpencV. When a user enters the ATM kiosk,first the upperbody is detected and then the face. Face Recognition is then performed. If the user already exists in the database the frequency count is incremented. Otherwise a new row is added to the databse with the id of the new user, his frequency, image path and the timestamp. When the frequency becomes greater than or equal to 4 an alert will be sent to the bank officials.If the same person enters the kiosk more than once within the 20 minutes an alert will be sent.Also if the face or the eyes of the person is covered then also an alert is sent to the officials.The Application contains a webpage which stores the log of the alerts that has been sent to the bank officials.Through the webpage live feed from the camera can also be viewed.
With the help of this application there is no need to manually watch the ATM for any suspicious activities.With the help of this application it can be automated which helps to save time and make the work for easy.Even if the bank officials are not able to hear the alert at that time,with the help of the log index they can know the time when each alert was issued and why.

Chapter 12

Future Scope

This project presents an automated system to increase the security and surveillance of ATM kiosks. Due to the increase of robbery in ATM kiosks, it is important to employ an automated surveillance system to protect and secure the ATM machine from threats. Currently, a camera attached with the ATM unit, records and transmits the video feed to the main server of the bank. Around the clock, this manual surveillance utilizes a lot of bandwidth for transmission. There is waste of memory and late response to emergency situation. Consequently, early detection of the situation is necessary to take preventive measures against an ongoing burglary.
With an automated surveillance system, it is possible to detect whether a person is wearing a mask or not. The proposed system is also capable of counting the number of people present inside the ATM kiosk and generate a warning signal, thereby removing constant human supervision, reducing the storage of unnecessary video feed and transmitting only an anomalous situation.

References

[1] http://www.academia.edu/26626901/Face_Detection_and_Recognition_Theory_and_Practice_eBookslib/

[2] https://facedetection.com/algorithms/

[3] htts://algorithmia.com/algorithms/opencv/FaceDetection

[4] Kernel Construction for Face Recognition by Jun-Bao Li, Shu-Chuan ChuJeng-Shyang Pan